

EPA Data and Voice Enterprise Network Services

Attachment J.3.7 – Statement of Work

GS00Q17NSD3000/68HERD22F0007



Table of Contents

C	EPA EIS Statement of Work	7
C.1	Purpose	7
C.2	Services Sought.....	8
C.3	Project Title.....	9
C.4	Project Overview.....	9
C.5	Project Goals	9
C.6	Description of Current Environment	11
C.6.1	Overview.....	11
C.6.1.1	Current Enterprise Wide Area Network Architecture	12
C.6.1.2	Current MTIPS Architecture	15
C.6.1.3	Current Enterprise Voice Services	21
C.7	Technical Requirements	24
C.7.1	Data Services Tasks	24
C.7.1.1	Virtual Private Network Service (VPNS).....	24
C.7.1.1.1	Connectivity	25
C.7.1.1.2	Standards	25
C.7.1.1.3	Technical Capabilities	25
C.7.1.1.4	Features.....	26
C.7.1.1.5	Interfaces	26
C.7.1.1.6	Performance Metrics	26
C.7.1.1.7	VPNS Special Requirements	26
C.7.1.2	Ethernet Transport Service (ETS).....	27
C.7.1.2.1	Connectivity	28
C.7.1.2.2	Standards	28
C.7.1.2.3	Technical Capabilities	28
C.7.1.2.4	Features.....	28
C.7.1.2.5	Interfaces	28
C.7.1.2.6	Performance Metrics	28
C.7.1.3	Private Line Service (PLS).....	28
C.7.1.3.1	Connectivity	29
C.7.1.3.2	Standards	29
C.7.1.3.3	Technical Capabilities	29
C.7.1.3.4	Features.....	29
C.7.1.3.5	Interfaces	29

C.7.1.3.6	Performance Metrics	29
C.7.1.4	Internet Protocol Service (IPS).....	30
C.7.1.4.1	Connectivity	30
C.7.1.4.2	Standards	30
C.7.1.4.3	Technical Capabilities	31
C.7.1.4.4	Features.....	31
C.7.1.4.5	Interfaces	31
C.7.1.4.6	Performance Metrics	31
C.7.2	Voice Services Tasks.....	31
C.7.2.1	Internet Protocol Voice Service (IPVS)	31
C.7.2.1.1	Connectivity	32
C.7.2.1.2	Standards	32
C.7.2.1.3	Technical Capabilities	32
C.7.2.1.4	Features.....	44
C.7.2.1.5	Interfaces	44
C.7.2.1.6	Performance Metrics	44
C.7.2.1.7	Managed LAN Service / Optional	44
C.7.2.1.8	Session Initiation Protocol (SIP) Trunk Service / Optional	44
C.7.2.2	Circuit Switched Voice Service (CSVS).....	45
C.7.2.2.1	Connectivity	45
C.7.2.2.2	Standards	46
C.7.2.2.3	Technical Capabilities	46
C.7.2.2.4	Features.....	46
C.7.2.2.5	Interfaces	47
C.7.2.2.6	Performance Metrics	47
C.7.2.2.7	CSVS Special Requirements	47
C.7.2.3	Toll Free Service (TFS).....	47
C.7.2.3.1	Connectivity	48
C.7.2.3.2	Standards	48
C.7.2.3.3	Technical Capabilities	48
C.7.2.3.4	Features.....	49
C.7.2.3.5	Interfaces	49
C.7.2.3.6	Performance Metrics	49
C.7.2.4	Circuit Switched Data Service (CSDS).....	50
C.7.2.4.1	Connectivity	50

C.7.2.4.2	Standards	51
C.7.2.4.3	Technical Capabilities	51
C.7.2.4.4	Features.....	51
C.7.2.4.5	Interfaces	51
C.7.2.4.6	Performance Metrics	51
C.7.3	Managed Services Tasks.....	51
C.7.3.1	Managed Network Service (MNS).....	51
C.7.3.1.1	Connectivity	53
C.7.3.1.2	Standards	53
C.7.3.1.3	Technical Capabilities	54
C.7.3.1.4	Features.....	54
C.7.3.1.5	Interfaces	54
C.7.3.1.6	Special Requirements	55
C.7.3.1.7	Performance Metrics	60
C.7.3.2	Managed Trusted Internet Protocol Service (MTIPS)	61
C.7.3.2.1	MTIPS Locations.....	61
C.7.3.2.2	Connectivity	61
C.7.3.2.3	Standards	61
C.7.3.2.4	Technical Capabilities	61
C.7.3.2.5	Features.....	64
C.7.3.2.6	Interfaces	64
C.7.3.2.7	Performance Metrics	64
C.7.3.2.8	Special Requirements	64
C.7.3.3	Managed Security Services	65
C.7.3.3.1	Distributed Denial of Service (DDoS) Defense Service.....	65
C.7.3.3.2	Secured Email Gateway Service	66
C.7.3.3.3	Security Operations Center (SOC) Managed Security Services	67
C.7.3.3.4	Performance Metrics	68
C.7.4	Access Arrangements Tasks	71
C.7.4.1	Connectivity	72
C.7.4.2	Standards	72
C.7.4.3	Technical Capabilities.....	72
C.7.4.4	Access Diversity and Avoidance	72
C.7.4.4.1	Research Triangle Park Access Diversity and Avoidance	72
C.7.4.5	Interfaces.....	73

C.7.4.6	Special Requirements.....	73
C.7.4.6.1	Broadband and Cellular Access Arrangement.....	73
C.7.5	Cable and Wiring Service (CWS) Tasks.....	73
C.7.5.1	Special Requirements.....	74
C.7.5.2	Performance Metrics.....	77
C.7.6	Service-Related Equipment (SRE) Tasks	78
C.7.7	Service-Related Labor Tasks	79
C.7.8	System Security Requirements/Tasks.....	79
C.7.8.1	System Security Compliance Requirements	79
C.7.8.2	Security Compliance Requirements	79
C.7.8.3	Security Assessment and Authorization (Security A&A).....	79
C.7.8.4	System Security Plan (SSP)	79
C.7.8.5	System Security Plan Deliverables	80
C.7.8.6	Additional Security Requirements	80
C.7.8.7	Personnel Background Investigation Requirements	80
C.7.8.8	Protection of Government Property.....	80
C.7.8.9	Personnel Security Clearances.....	81
C.7.9	National Policy Requirements Tasks.....	81
C.7.9.1	National Security and Emergency Preparedness	81
C.7.10	Technical Support Tasks.....	81
C.8	Transition Tasks.....	81
C.8.1	Transition Roles and Responsibilities.....	81
C.8.1.1	Government's Role in Transition	81
C.8.1.2	Contractor's Role in Transition	82
C.8.2	Transition On Tasks.....	82
C.8.2.1	Transition Approach.....	82
C.8.2.1.1	Transition Gateway	82
C.8.2.2	Transition Team Organization	83
C.8.2.3	Governance and Reporting	84
C.8.2.4	Quality Control	84
C.8.2.5	Communications	84
C.8.2.6	Workforce Transition.....	84
C.8.2.7	Work Execution During Transition.....	84
C.8.2.8	Subcontracts.....	84
C.8.2.9	Property Transition	84

C.8.2.9.1	Government Furnished Equipment (GFE)	84
C.8.2.9.2	Incumbent Owned Equipment	85
C.8.2.9.3	Intellectual Property	85
C.8.2.10	User Accounts and Passwords	85
C.8.2.11	Knowledge Transfer	85
C.8.2.12	Potential Risks	85
C.8.2.13	Schedule	85
C.8.2.14	Handover and Acceptance	86
C.8.3	Transition Off Tasks	86
C.9	Section 508 Requirements/Tasks	86
C.9.1	Background	86
C.9.2	Voluntary Product Accessibility Template	86
C.9.3	Section 508 Applicability to Technical Requirements	86
C.9.4	Section 508 Provisions Applicable to Technical Requirements	87
C.9.5	Section 508 Provisions Applicable to Reporting and Training	87
C.9.6	Operating Constraints	87
C.10	Technology Refresh Tasks	87
C.11	Program Management Tasks	88
C.11.1	Meetings	88
C.11.2	Program Management Plan (PMP)	88
C.11.2.1	Management Approach and Governance Model	89
C.11.2.2	Resource Management	89
C.11.2.3	Risk Management	90
C.11.2.4	Services Verification Testing	91
C.11.2.5	Training	91
C.11.2.6	Reporting	91
C.12	EPA CIO Directives	92

C EPA EIS Statement of Work

This is the Environmental Protection Agency (EPA) Statement of Work (SOW) for services utilizing the General Services Administration's (GSA) Enterprise Infrastructure Services (EIS) contract.

The baseline requirements for the services sought herein are defined in Section C of the *EIS Contract*. The EPA expects that all *EIS Contractors* provide the baseline level of service as defined in the *EIS Contract*. The EPA has additional, agency-specific requirements that are described in this SOW. This SOW describes the full range of mandatory and optional services required by EPA. EPA plans to award the telecommunications services listed as mandatory services. Those identified as optional here and within the Pricing Workbook in J.1, must be priced by the Contractor, and may or may not be ordered in a future Task Order by the EPA.

The *EIS Contractors* shall provide all personnel, transportation, equipment, tools, materials, supplies, installation, management, supervision, engineering, maintenance, testing, and services necessary to make circuits/services fully operational and to perform all tasks and functions as defined in this SOW.

The scope of the awarded TO(s) includes all baseline services being transitioned to EIS with required or optional current network functionality described in this SOW, as well as future capabilities offered through the EIS program that will replace or improve that functionality. Consistent with Section C.2.11 of the *EIS Contracts*, the *EIS Contractors* shall provide, at no additional cost to the government, all service-related labor necessary to implement the services. The *EIS Contractors* shall deliver any Service-Related Equipment (SRE) necessary to implement and manage any of the services.

The Contractor shall adhere to the terms and conditions specified in the EIS Contract in addition to the service specific requirements in this solicitation. Note that this solicitation may contain requirements supplemental to those defined in the EIS Contract. The Contractor is responsible for recognizing and supporting those supplemental requirements

C.1 Purpose

The purpose of this SOW is to provide the EPA with a contractual vehicle to transition its telecommunications services from the GSA Networkx, GSA WITS 3, and GSA Regional contracts to the GSA Enterprise Infrastructure Solutions (EIS) contract for the continuity of telecommunications services for the agency.

The mission of the EPA is to protect human health and the environment. The agency works to ensure that:

1. Americans have clean air, land and water;

2. National efforts to reduce environmental risks are based on the best available scientific information;
3. Federal laws protecting human health and the environment are administered and enforced fairly, effectively and as Congress intended;
4. Environmental stewardship is integral to U.S. policies concerning natural resources, human health, economic growth, energy, transportation, agriculture, industry, and international trade; and these factors are similarly considered in establishing environmental policy;
5. All parts of society--communities, individuals, businesses, and state, local, and tribal governments--have access to accurate information enough to effectively participate in managing human health and environmental risks;
6. Contaminated lands and toxic sites are cleaned up by potentially responsible parties and revitalized; and
7. Chemicals in the marketplace are reviewed for safety.

The agency's information technology (IT) infrastructure supports the missions of the agency's ability to communicate, collaborate, and partner with communities, individuals, businesses, state, and local governments to fully protect human health and environment through education utilizing scientific information, establishment of environmental policies, and enforcement of federal laws.

To ensure the continuity of its IT infrastructure, the agency will transition the GSA Network, GSA WITS, and GSA Regional Contracts circuits and services to the GSA *EIS Contract*, whereas the agency anticipates an initial like-for-like transition for its items that are presently on the GSA Network, GSA WITS 3, and GSA Regional Contracts.

C.2 Services Sought

EPA seeks to acquire the telecommunications services listed below which are mandatory. Those identified as *optional* here and within Section J.1 Pricing Workbook must be priced by the Contractor but may or may not be ordered in a future Task Order.

Data Services:

- Virtual Private Network Service (VPNS)
- Ethernet Transport Service (ETS)
- Private Line Service (PLS)
- Internet Protocol Service (IPS)

Voice Services:

- Internet Protocol Voice Service (IPVS)

- Circuit Switched Voice Service (CSVS)
- Toll Free Service (TFS)
- Circuit Switched Data Service (CSDS)

Managed Services:

- Managed Network Service (MNS)
 - Data MNS
 - Voice MNS – *Optional*
 - Software Defined Wide Area Network (SDWANS) - *Optional*
- Managed Trusted Internet Protocol Service (MTIPS)
- Managed Security Service (MSS)
 - Distributed Denial of Service (DDoS) MSS
 - Secure Email Gateway MSS
 - Security Operations Center (SOC) MSS

Access Arrangements (AA)

Service Related Equipment (SRE)

Service Related Labor (LABOR)

Cable and Wiring Service (CWS)

National Security and Emergency Preparedness (NS/EP)

C.3 Project Title

EPA Data and Voice Enterprise Network Services

C.4 Project Overview

The agency will execute a successful, timely, and orderly transition of all the agency's telecommunications and information technology services from the expiring GSA Networkx, GSA WITS 3, and GSA Regional contracts to the new GSA Enterprise Infrastructure Solutions (EIS) contract. The migration from the GSA Networkx, GSA WITS 3 and GSA Regional contracts to the GSA Enterprise Infrastructure Solutions contract will be complete no later than September of 2022.

C.5 Project Goals

EPA is committed to a service-oriented approach to network design, maintenance, support, and building services with an EIS provider that is aligned with the agency's expectations. The EPA's expectation is that the Contractor shall implement like-for-like versions of the agency's current services by acting as the integrator of the proposed technical solution. The agency believes that

using this approach along with making provisions to implement optional modernization technology initiatives will result in a network design that delivers an increased value to the agency's community while minimizing transition risk. The Contractor's solution shall be a conduit for using technology to enable the mission of the agency by focusing on business-centric activities. The basic objectives for this SOW are centered around a customer focused IT service delivery approach in four areas; meeting customer expectations for IT services, achieving customer goals for cost-effective services, providing IT steady state processes, and achieving proactive management and innovation in the IT services that the Contractor shall provide through the life of the contract.

The agency believes that Customer IT Service expectations shall be satisfied by delivering superior design and performance characteristics in the areas of superior service availability, scalability, network performance, security, manageability, usability, and adaptability. Those characteristics are further defined in the Table C-5 Customer IT Service Expectations below.

Table C-5, Customer IT Service Expectations

Customer IT Service Expectations	
Performance Characteristics	Definition
Availability	Minimizes unscheduled outages and reduces the number of scheduled outages, overall design shall provide for resiliency and load-balancing capabilities
Scalability	A network design that is simplified yet modular
Network Performance	A network design that meets or exceeds current thresholds as stated on the <i>EIS Contract</i>
Security	Ensures an optimal level of security
Manageability	Complement the network management model allowing for performance, fault, configuration, security and accounting management. The technical solution is designed in concert with the fault management approach to detect, isolate, and correct problems in adherence to ITIL standards
Usability	Seamless network access by users, independent of location
Adaptability	A design that has the flexibility to adjust when needed, based on EPA's continual improvement cycle in a timely fashion. The design is flexible and adaptable, to meet emergency operations requirements.

Affordability	Both the costs and the benefits of the products and services chosen are weighed as part of the technical solution, to choose a design that meets the agency's objectives and represents the best value for the agency.
---------------	--

The Contractor shall deliver a steady state IT services that demonstrates the ability to transition to an EIS solution that provides day-to-day operational stability, flexible solution service integration, and security compliance with demonstrated processes and procedures providing an effective metric management. EPA expects that the Contractor shall provide scalable capacity and superior performance with improved response times to deliver solutions. EPA expects that the Contractor shall provide the agency customers with a reduced time to select, assess, and deploy newer technologies and enhancements to the existing infrastructure. EPA expects that the Contractor shall leverage the Contractor's experience with other agencies to keep pace with emerging technologies and provide faster integration of these technologies into the agency's network infrastructure.

EPA expects that the Contractor shall improve the quality of support that customers receive by reducing the time required to resolve problems by improving support infrastructure. In addition, EPA expects that the EIS migration from Networx requires the need for superior project management of the transition, transition from existing network circuit provisioning, and support to migrate to the EIS solution. During this transition, EPA expects that the Contractor will develop a partnership with EPA to better understand the agency's changing requirements, as well as to provide leadership in technology and management solutions that introduce greater value to the agency, while minimizing any downtime and disruption of network services to the agency customers.

EPA expects that the Contractor designs shall have the flexibility to adjust when needed, based on the agency's continual improvement cycle, or for an emergency operational requirement, in a timely fashion, without service disruption or degradation. Those designs shall have the capability to incorporate such future modernization objectives such as, Software-Defined WAN (SD-WAN) as an overlay and SIP Trunking, which are both optional services for the agency.

C.6 Description of Current Environment

C.6.1 Overview

This section describes the basic architecture of the agency network and is the services provided and utilized from the GSA Networx, GSA WITS 3, and GSA Regional Contracts that comprise the current voice and data enterprise network services for the EPA.

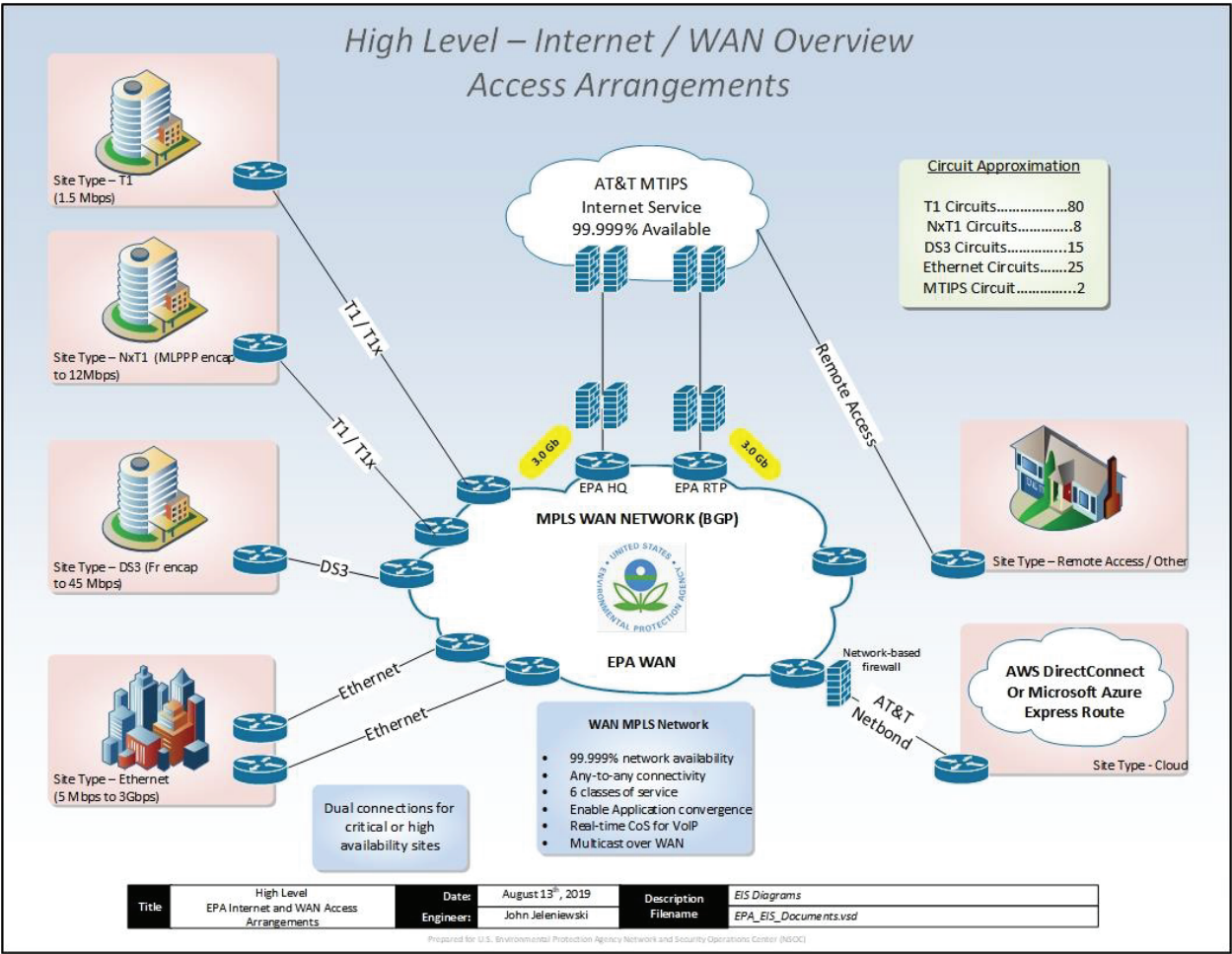
C.6.1.1 Current Enterprise Wide Area Network Architecture

The Enterprise Wide Area Network (EWAN) is an EPA General Support System (GSS) that is comprised of several systems supporting areas including services, systems and applications. These areas are broken down into the following:

- Wide Area Network (WAN) and Local Area Networks (LAN) that interconnect all the EPA office locations, as well as the two Internet connections provided through the GSA Networkx Provider Managed Trusted Internet Protocol Service (MTIPS).
- Systems/Applications supporting the agency's Enterprise Wireless Network;
- DDI (DHCP, DNS and IPAM) systems and services supporting all the agency's locations and program offices;
- Security systems and services that provide boundary protection and authentication services to control access to various systems (i.e. Firewalls, TACACS+, etc.);
- Remote Access systems and services that allow users to connect to EPA systems and applications;
- Supporting tools that allow the Network and Security Operations (NSO) and Local Area Network Enterprise Services (LANES) Task Orders (TOs) to perform daily operational activities.

In Figure 1: High Level - Internet / WAN Overview, a graphic representation of the IP/MPLS converged managed network solution has been provided and in this graphic representation, the agency's sites of varying bandwidths connected to the NBIP-VPNS network are depicted, with two separate diverse connections to the agency's Washington, DC, and Research Triangle Park sites into MTIPS portals with associated security and MNS services provided from the GSA Networkx Provider's Network Operations Center (NOC).

Figure 1: High Level – Internet / WAN Overview



This drawing illustrates examples of the managed sites with: Standard offices (T1-NxT1), Medium offices (fractional DS3 to DS3), Large office bandwidth (OC3 and OC12), and Very high bandwidth (aka OC48 or greater), as well as illustrating a typical location at the agency utilizing Ethernet services for access into the NBIP-VPNS.

The Premise-Based IP VPN (PBIP-VPN) illustrates the agency's Remote Access capabilities and allows the agency to use shared Internet technology, rather than leased lines, to conduct federal business. The PBIP-VPN service provides dedicated broadband and remote access connections to the Internet.

The EPA WAN and EPA LAN are in a distributed environment across the EPA's approximately 100 locations. Each Regional Office, Program Office, Headquarters, and Laboratory have at least one managed router connecting the site to the WAN and switches providing the LAN component. Field Offices, Continuity of Operations (COOP) sites, and other remote locations

may also have small managed routers connecting to the WAN. The WAN is an IP based/MPLS converged managed network solution that is built on the enterprise network built on services from the GSA Networkx service offerings Network Based IP VPN (NBIP-VPNS), Managed Trusted IP Services (MTIPS), Managed Network Services (MNS), and Service Enabling Devices (SED). The WAN and LAN devices are products of Cisco Systems, Inc. Local circuits provided by the GSA Networkx Provider attach the routers at each of about 100 sites to the WAN “Cloud” provided by GSA Networkx Provider. This cloud is configured in a Layer 2 and Layer 3 Multi-Protocol Label Switching (MPLS) configuration. The network infrastructure supports a broad variety of both custom and off-the-shelf applications for VoIP delivery, Video delivery, dual Internet gateways, and publicly accessible content such as www.epa.gov, and the Central Data Exchange (CDX), which provides a reporting platform for receiving data from individuals, states, and countries outside of the enterprise network.

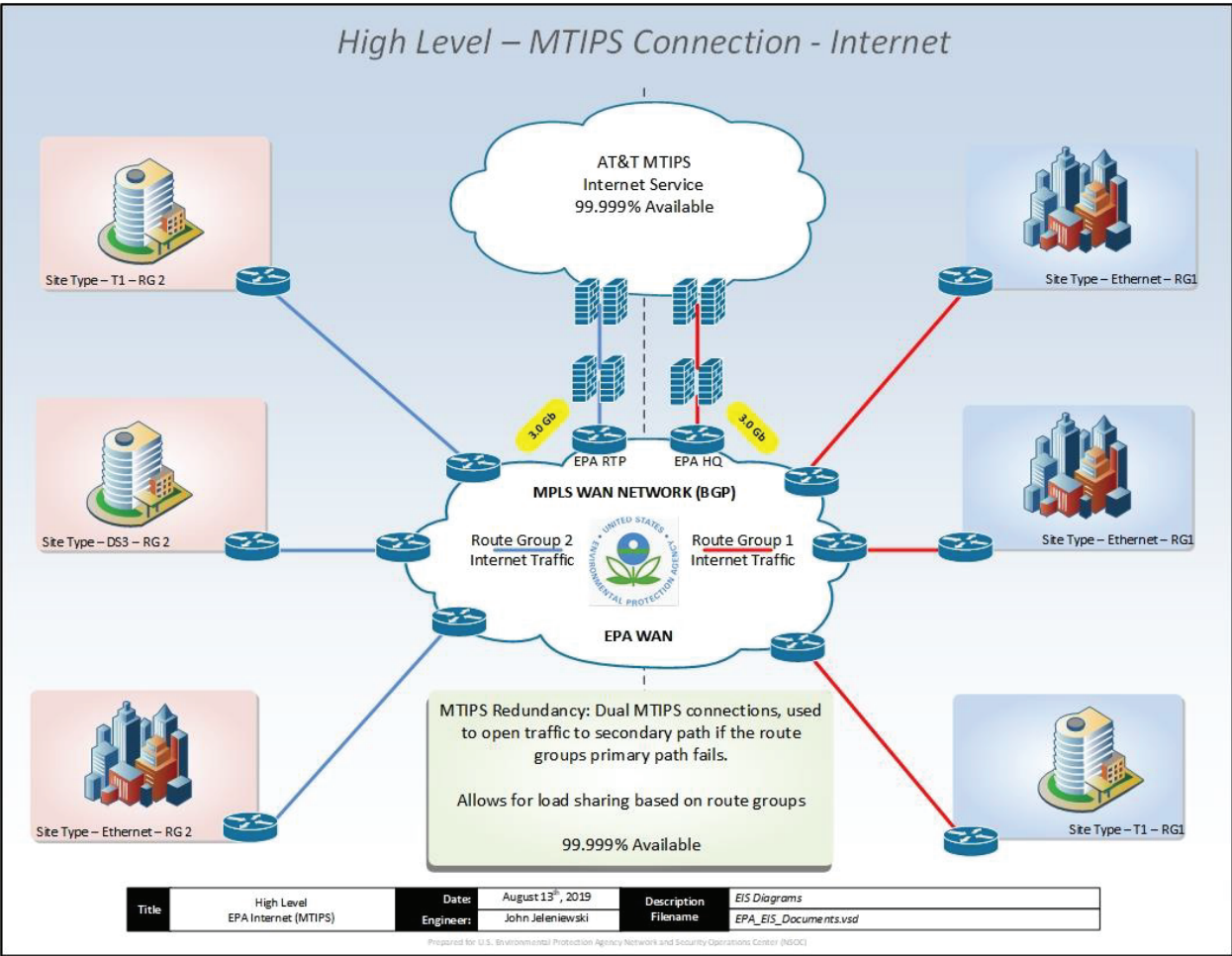
Circuits supporting the agency’s connection to the VPNS are connected via traditional TDM circuits as well as Ethernet access. Where available, Ethernet access service is the preferred transport method. As an example, a Region may consist of a mixture of T1, MLPPP, fractional DS-3, as well as higher-speed Ethernet circuits. Each transport type is deployed with only a single connection to VPNS, either via frame-relay PVC, PPP, or 802.1Q VLAN. The solution provided leverages the GSA Networkx CLINS to include the ETS, IPS, and VPNS Services. Each location on the WAN is connected via a Cisco router which terminates the VPNS circuit. Password-protected analog modems are connected to the router’s console ports to allow remote troubleshooting following the failure of the connected WAN circuit. Routers are monitored by the Service Provider under the Managed Network Services for Data. The LAN consists of network devices (switches and routers) that are in the data centers and regional/program offices throughout EPA, to provide connectivity of end devices (laptops, servers, printers, scanners, telephones, etc.). At each agency location, the WAN router is the interface point between the WAN and the LAN. The LANs are Ethernet based and supported directly by EPA personnel or Contractors.

All remote locations housing EPA’s WAN/LAN components are governed by recommendations for physical security and environmental conditions. Physical security is the responsibility of the Office of Administration and Resources Management (OARM), Administrative Services Division (ASD), regional organizations, and program offices. Administrative Services Division (ASD) provides the guard force, badge reader system, and procedures required to operate the building in accordance with Federal, Agency, and NCC requirements. The WAN and LAN complies with the security specifications defined in the Environmental Protection Agency Information Security Policy. CIO Directive 2150.3. Industry Best Practices and Standard Industry Architecture are applied to the network implementation.

C.6.1.2 Current MTIPS Architecture

As depicted in Figure 2, EPA is presently utilizing the GSA Networkx Contract for the Managed Trusted Internet Protocol Service (MTIPS). The current performance standards in place are dictated by the GSA Networkx Contract for the Managed Trusted Internet Protocol Service (MTIPS) provided for the Service Level Requirements. The Managed Trusted Internet Protocol Service (MTIPS) provided under the GSA Networkx Contract allows the subscribing agency to logically connect to the public Internet or other external connections, as required by Federal Regulatory directives, using a Trusted Internet Connection (TIC) portal. The TIC Portal functions as a Multi-Service Trusted Internet Connection Access Provider (TICAP). The TIC portals for the agency are located in Washington, DC, and the National Computer Center (NCC) in Research Triangle Park, North Carolina. The GSA Networkx Provider has dual 10GB Ethernet circuits from the TIC portal to the Internet (north bound side) and from the TIC portal to the GSA Networkx Provider MPLS cloud (south bound side). Customer traffic is load-shared across the two circuits at less than 50% peak loading on an individual circuit, so that either circuit can handle the full load of traffic should the other circuit fail. Per TIC requirements, each of the circuits on the north side are routed diversely and terminates in the geographically dispersed POPs. The GSA Networkx Provider MTIPS solution incorporates built-in redundancy to include partial and complete automated failover to the remaining MTIPS assets. In addition, each of the GSA Networkx Provider facilities chosen has contingency and/or disaster recovery mechanisms in place to provide the redundancy for each TIC portal to monitor and manage the capabilities of the other. MTIPS systems/applications/services are considered critical and, as such, replicate data every two minutes in the event of a major failure. Each of these components are shown in Figure 2: Managed Trusted Internet Protocol Service (MTIPS) Solution. The National Computer Center (NCC) located at Research Triangle Park (RTP) has dual 2Gb/sec Ethernet connections to the WAN which are delivered via the diverse 10Gb fiber paths onto the campus. These circuits provide redundancy for one another as well as local diversity for the site. These circuits also connect to separate facilities on the RTP Campus (NCC and Campus C-Building) and are served by a separate local telco point of presence (POP). These circuits carry all public-content data being provided by agency's sites and Internet service for Regions 6-10. The William Jefferson Clinton (WJC) location provides identical WAN and Internet connectivity as compared to the NCC, but also supports Internet service for Regions 1-5 as well as being the secondary data center located at Potomac Yards (PY) in Arlington, Virginia.

Figure 2: Managed Trusted Internet Protocol Service (MTIPS) Solution



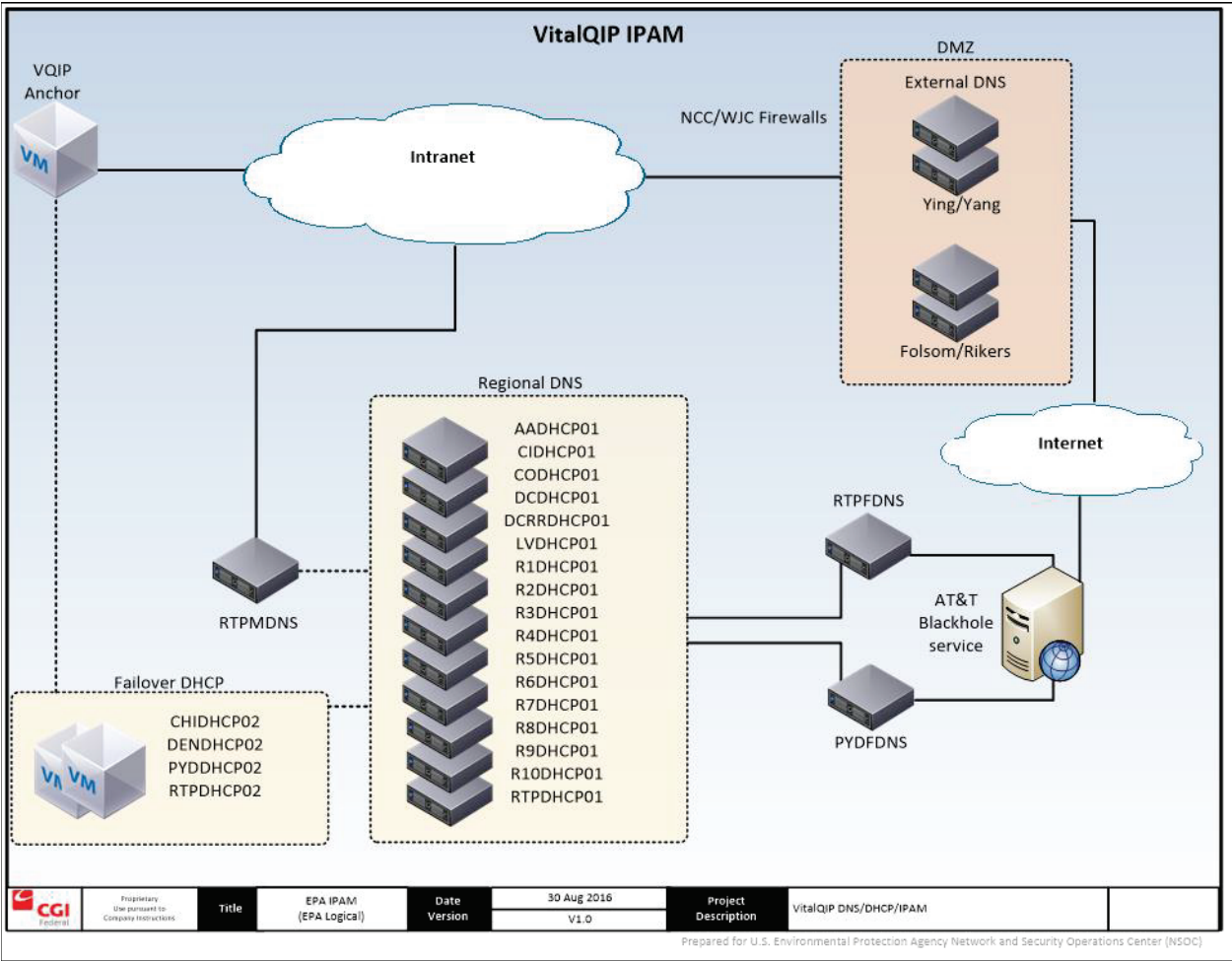
The Managed Trusted Internet Protocol Service (MTIPS) solution provides the following features to the agency; caching, DNSSEC verification, URL filtering/white lists/black lists, proxy services, transparent (HTTP), explicit (HTTPS), HTTPS active content filtering, firewalling, intrusion detection service, ability to implement custom signatures, anti-virus/anti-malware, secure email gateway, secure email filtering, Stateful Packet Inspection, packet capture, enforcement of agency-specific sender authentication policies using both Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM) technology, and an threat management solutions that includes event generators (appliances and applications) that scan and/or interrogate all agency inbound and outbound traffic, and storage of all data events, communicated to the agency via secure, web-based portal, reporting, accessed via secure, web portal, firewall, URL and IDS data presented, and participation in NCPS (formerly known as EINSTEIN). In addition, the GSA Networkx Provider MTIPS solution provides and performs virus

and anti-spam scanning for SMTP (port 25/tcp) traffic using Fortinet FortiMail, which the Service Provider refers to as the Secure Email Gateway (SEG).

The EPA Enterprise Wireless Solution allows the EPA to authenticate, authorize, and audit wireless users and devices attaching to the network. The wireless network supports EPA GFE devices allow access to internal and external systems and guest devices that are only permitted to reach Internet based systems.

EPA utilizes the Nokia VitalQIP® product to provide domain name system (DNS), Dynamic Host Configuration Protocol (DHCP) and IP address management (DDI). This product incorporates management to configure, automate, integrate, and administer DDI services across EPA's entire IP network. shows the current DNS and DHCP systems.

Figure 3: VitalQIP IPAM



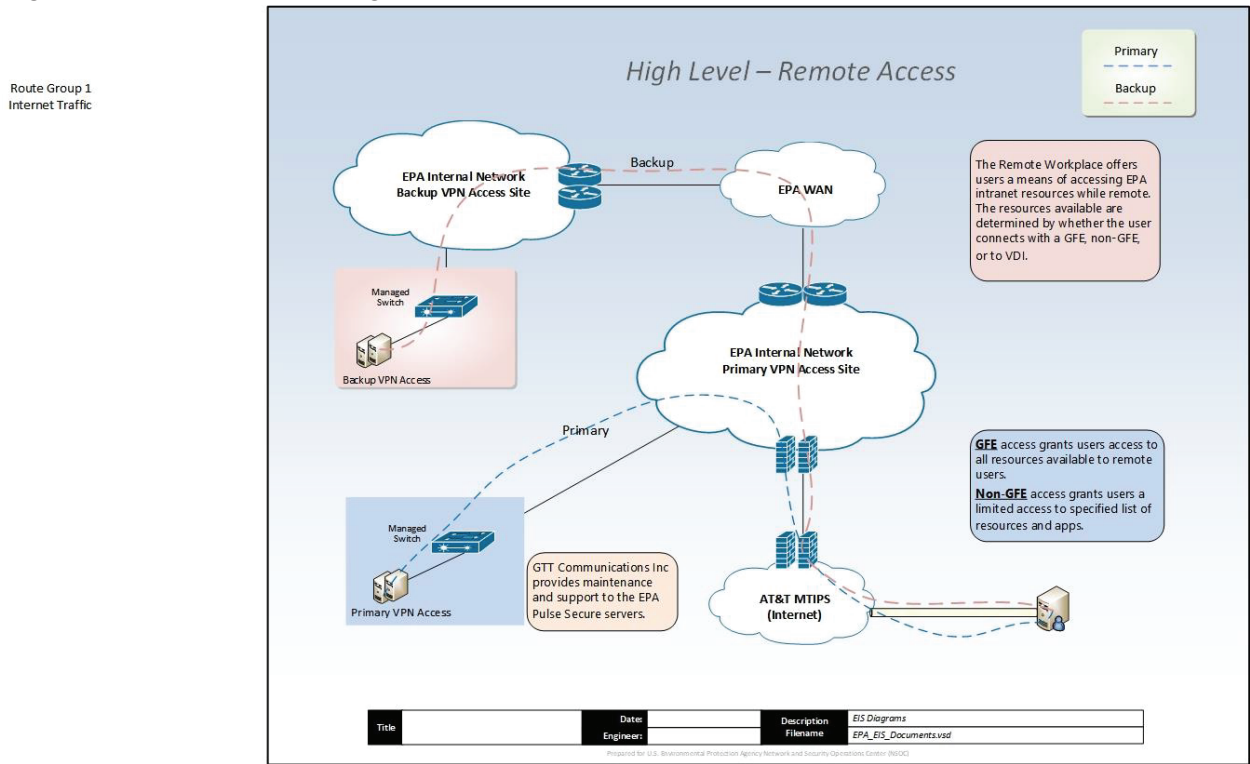
The core systems of this infrastructure are in the RTP National Computer Center (NCC), the Potomac Yards Data Center, and end user supporting systems that are distributed throughout the agency's regional and program office locations.

The EWAN utilizes several security systems to provide the EWAN with proper security protection. The systems included are: FortiGate and CheckPoint firewalls: The EWAN manages six FortiGate firewalls (two in NCC for the MTIPS connection, two in WJC for the MTIPS connection, and two in PYD for enclave protection). The EWAN GSS supports two FortiGate firewalls for the Office of Pollution Prevention and Toxics (OPPT) and two CheckPoint firewalls for the Fingerprint Transmission System (FTS). The EWAN manages four Cisco ACS TACACS+ servers that provide AAA services for Cisco routers and switches in EPA locations for EWAN; the NAC PRIME system; the Gigamon system; the network jump boxes Stargate and Destiny, and the Cisco ISE system: The TACACS+ authentication system provides Authentication, Authorization and Accounting (AAA) services for network routers and switches throughout the agency.

DNS is administered internally and provides support for more than 70 top-level-domains (TLDs). The Network Admission Control (NAC) solution is a sub-component of the EPA's Enterprise Wide Area Network (EWAN) General Service System (GSS). The Network Admission Control (NAC) referenced refers to Cisco's version of Network Access Control, which restricts access to the network based on identity or security posture. The NAC System includes (3) major CISCO components: the Mobility Services Engine (MSE), Identity Service Engine (ISE), and the Cisco PRIME platform. The Cisco MSE is a platform that enables the wireless network to deliver mobility services in a centralized and scalable way. The Cisco Identity Services Engine delivers all the necessary services required by enterprise networks—AAA, profiling, posture, and guest management—on a common platform. Cisco PRIME provides converged user, access, and identity management across wired and wireless networks Users that attach to the EPA wireless network will use the NAC system for authentication and access control to EPA resources.

This Managed Secure Access Service is a Premise-Based IP VPN (PBIP-VPN), utilizing an SSL VPN system that is composed of the GSA Networkx Provider Network Operations Center (NOC) and the Customer Premise Equipment (CPE) located in Potomac Yard at Arlington, Virginia and the Customer Premise Equipment (CPE) located in National Computer Center (NCC) at Research Triangle Park, North Carolina. The CPE contains an SSL VPN appliance and management device. The GSA Networkx Provider NOC provides the management tools and services to manage the CPE that make up the Secure Access System (SAS). Please refer to Please refer to Figure 4: Remote Access High Level.

Figure 4: Remote Access High Level



The GSA Networkx Provider provides to the agency, (i) use of the CPE installations, (ii) access to and use of the Service Providers SSL VPN software modules, (iii) management, support and monitoring of the agencies Secure Access Service (SAS) from the Service Providers NOC and (iv) access to the Service Management Console. The GSA Networkx Provider NOC provides 24x7x365 telephone and email support, management, monitoring and availability reporting of the SSL VPN system.

The current SAS hardware configuration is provided by two (2) high availability level CPE that includes two (2) SSL VPN appliance nodes that are configured for an 99.9% SLA. The current SAS hardware configuration can support up to 25,000 concurrent remote users per location. A Test SSL VPN Server is in the National Computer Center (NCC). The purpose of the Test Server is to create agency specific policies, test polices, certify configurations, and then implement an agency profile into the production environment. This Test Server mimics the configuration of the supplier production CPE, insofar as needed to stage agencies in a pre-production environment. The current SAS software configuration will support 7,500 concurrent remote users.

In the two tables below, Table 1: Equipment Deployed by Location and Table 2: Managed Secure Access Service - Appliance, License, & Maintenance additional information is provided for the configuration.

Table 1: Equipment Deployed by Location

Equipment Deployed by Location				
Potomac Yard 2777 Crystal Drive Arlington, VA 22202	Model	Units	Form Factor	Ports Required Internal/External
Pulse Secure TLS Gateway	PSA7000	2	2RU	3 Internal / 4 External
WTI - Remote Power Unit	RSM-8R8-1	1	1RU	
Iron System Admin Server	CS-MEG	1	1RU	
RTP – NCC 109 TW Alexander Drive RTP, NC, 27711	Model	Units	Form Factor	Ports Required Internal/External
Pulse Secure TLS Gateway	PSA7000	2	2RU	3 Internal / 4 External
Pulse Secure TLS Gateway	PSA3000	1	1RU	
WTI - Remote Power Unit	RSM-8R8-1	1	1RU	
Iron System Admin Server	CS-MEG	1	1RU	

Table 2: Managed Secure Access Service - Appliance, License, & Maintenance

Managed Secure Access Service Appliances, License, & Maintenance Contracts			
Service Description	Item Code	Location	
CPE Mgmt. - HA Pulse Secure PSA7000 - Support up to 25,000 Concurrent Users	CPEM-PSA- 7000-HA	DC, USA	
CPE Mgmt. - HA Pulse Secure PSA7000 - Support up to 25,000 Concurrent Users	CPEM-PSA- 7000-HA	NC, USA	
License Server Management & Global Concurrent Licenses - 7,500	CPEM-PSA- 7500CC	Cloud	

To provide day-to-day operational support for the EWAN, the Task Order's assigned to this GSS utilize various tools installed on EPA servers and appliances that provide such functions as monitoring, alerting, system access, and configuration management. The EWAN uses several tools to provide monitoring, management, and alerting to the support groups. The following are the major tools, which include but are not limited to, used by the EWAN: Network and Security Jump Boxes, Tenable Nessus, EWAN logging Systems, Plixer Scrutinizer, SolarWinds Network Configuration Manager, AlgoSec SRM system, ATLAS, Perspica, Net Line Dancer, Splunk, CISCO Prime, and EM-7.

The agency has migrated to the GSA Networkx Provider managed solution; Managed Network Services for Data to meet the agency requirements to include full life-cycle management of the network infrastructure, monitoring of telecommunications services, real-time and proactive network monitoring, troubleshooting, and service restoration. The GSA Networkx Provider for this managed service is the agency's single point of accountability for the agency networked services managed under this service, including operations, maintenance, and administration activities. The current performance standards for these services are dictated by the Task Order for the Service Level Requirements.

Access Diversity and Avoidance is implemented within the Research Triangle Park (RTP) facility. The National Computer Center (NCC) located at Research Triangle Park (RTP) has dual 2Gb/sec Ethernet connections to the WAN which are delivered via diverse 10Gb fiber paths onto the campus. These circuits provide redundancy for one another as well as local diversity for the site. These circuits connect to separate facilities on the RTP Campus (NCC and Campus C-building) and are served by separate local telco point of presence (POP). These circuits carry all public-content data being provided by agency's sites and Internet service for Regions 6-10. The William Jefferson Clinton (WJC) location provides identical WAN and Internet connectivity as compared to the NCC, but also supports Internet service for Regions 1-5 as well as being the secondary data center located at Potomac Yards (PY) in Arlington, Virginia.

EPA is presently utilizing the GSA Networkx, WITS, and Regional Contracts for Voice Services such as Circuit Switched Data Services (CSDS), Circuit Switched Voice Services (CSVs), and Toll-Free Services (TFS) throughout the CONUS and OCONUS locations of the EPA. The current performance standards that are currently in place for these services are dictated by either the GSA Networkx, WITS, or Regional Contracts for the Service Level Requirements.

C.6.1.3 Current Enterprise Voice Services

There are no Internet Protocol Voice Services (IPVS) or Managed Network Services for Voice (MNS) presently provided under the Networkx, WITS, or Regional Contracts. The agency owns the equipment that makes up the agency's own branded Enterprise Voice Services (EVS).

The Enterprise Voice Services (EVS) is an enterprise-wide telephony and voice mail system for the inter-agency and intra-agency voice traffic that utilizes PRI trunks for PSTN connectivity and currently does not utilize SIP trunks for PSTN connectivity.

The system is based on an Avaya Aura Telephony Platform consisting of the System Manager, Session Manager, Session Border Controller, Communication Manager, Aura Messaging, and Message Networking Server platform infrastructure hosted in EPA's Denver and Research Triangle Park Data Centers for H.323 and SIP telephony devices. Supporting network diagrams of the current Enterprise Voice Services (EVS) are provided in Section J.3.1.7, Research Triangle Park Network Diagrams and Section J.3.1.8, Denver Network Diagrams.

The Communication Manager and Aura Messaging are segregated into two different systems to serve different communities of users, the Research Triangle Park providing voice and voice mail services to the Headquarters, Cincinnati, Research Triangle Park, Mount Weather, OAR Montgomery, Office of Research and Development (ORD) Athens, and ORD Gulf Breeze locations and Denver providing voice and voice mail services to Region 1 through 10, OAR, CID, and ORD locations not previously identified as served by Research Triangle Park. The listing of the present locations served by the agency's own branded Enterprise Voice Services is given in Table 6 which includes the facility name, street address, city, state and zip code.

The Hosted Control for the Avaya Communication Manager at the Denver and Research Triangle Park Data Centers is an Avaya S87XX Media Server duplicated configuration at the Host Control locations. Two instances of the Avaya Communication Manager are active on the Avaya S87XX Media Servers duplicated configuration in the Denver and Research Triangle Park Data Centers. The Hosted Control in Denver and Research Triangle Park Data Centers are connected over the EPA MPLS WAN to each gateway on dedicated Layer 2 VLANs. The Hosted Control for the Avaya Aura Messaging at the Denver and Research Triangle Park Data Centers is three (3) Message Application Servers and one (1) Message Storage Server at the Host Control locations utilizing DL360 Servers. Each Hosted Control for the Avaya Aura Messaging at the Denver and Research Triangle Park Data Centers is connected to the Avaya Communication Manager at the Denver and Research Triangle Park Data Centers through three hundred (300) SIP trunks between the two systems.

The Hosted Control License Distribution for the Avaya Communication Manager and Avaya Aura Messaging are identified in Section J.3.1.2, Telephony and Voice Mail License Distribution for the Avaya Communication Manager and Avaya Aura Messaging for the Denver and Research Triangle Park Data Centers.

The gateways are configured for local survivability with Avaya S8300 Media Servers and Avaya DL360 servers at each gateway location. The Local Survivable Processor (LSP) is used if the communication link is broken between an Avaya Gateway and a Host Control, being the primary call controller. The determining factor on whether an Avaya S8300 Media Servers or/and the Avaya DL360 Server is used is based on the number of devices on the gateway. The LSP will provide service for the Avaya IP Telephones and H.248 Media Gateways that were controlled by the primary call controller. The LSP can be administered to either fail-back to the primary automatically or can be moved back manually.

Each location that is served by either an Avaya G430 or G450 Gateway(s) provides User Network Interface (UNI)'s including non-proprietary telephony analog station interfaces, non-proprietary telephony ISDN BRI station interfaces, and non-proprietary telephony PSTN access through ISDN PRI trunk interfaces on a per location basis.

The Avaya G430 or G450 Gateway supports various media modules providing connectivity to the PSTN with MM710 PRI Trunk and MM714 Central Office Trunk Media Modules. Section J.3.1.3, Gateway Configurations shows the equipped amount of PSTN interface modules in the gateway, and the pricing table contained in J.1, Pricing Spreadsheet shows the in-service PRI Trunks at each location.

Analog devices such as 2500 Telephones, 2554 Telephones, Auto dialers, etc. are connected to the platform with either an MM711 or MM716 analog module and is cross connected to the physical riser/feeder/station cabling at the location to the end device.

Video Conferencing devices or Secure Terminal Equipment (STE) are connected to the platform with the MM720 BRI/MM721 BRI module and is cross connected to the physical riser/feeder/station cabling at the location to the end device.

In Section J.3.1.3 Gateway Configurations, the non-proprietary telephony analog station interfaces, non-proprietary telephony ISDN BRI station interfaces, and non-proprietary telephony PSTN access through ISDN PRI trunk interfaces on a per location basis is given. The quantity of actual gateways and media modules is given as well as the capacity of the media modules. The quantity of IP Telephones is blank on this table, as they are shown on a per location basis in Section J.3.1.4 Site Telephone Inventory.

As shown in Section J.3.1.2 Telephony and Voice Mail License Distribution for the Avaya Communication Manager and Avaya Aura Messaging for the Denver and Research Triangle Park Data Centers, the amount of Communication Manager Licenses (27,881) provides licensing for telephony for the Analog and Basic Rate Interface (BRI) Stations as well as the IP Stations. Central Office Trunks and Primary Rate Interface Trunks do not require licensing in the Avaya Aura Platform. The IP Telephones identified in Section J.3.1.4 Site Telephone Inventory use the Communication Manager Licenses identified in Section J.3.1.2 Telephony and Voice Mail License Distribution for the Avaya Communication Manager and Avaya Aura Messaging for the Denver and Research Triangle Park Data Centers.

In these tables, Region 1 when compared with the Section J.3.1.1 Summary Telecom Inventory and Section J.3.1.3 Gateway Configurations would show that Region 1 encompasses the John W. McCormack Federal Building and the New England Regional Lab, Region 2 encompasses the Ted Weiss Federal Office Building, Edison Lab, and the Caribbean Environmental Protection Division, so forth and so on, etc.

Telephones are assigned on a per device basis through the Avaya Session Manager and Communication Manager infrastructure and voice mail is assigned on a per mail box basis through the Avaya Aura Messaging infrastructure hosted in the EPA's Denver and Research Triangle Park Data Centers from the System Administrators in the EPA's Headquarters' Offices,

Regions 1 through 10, Field Offices, OAR Labs, ORD Labs, OARM Cincinnati, OARM Research Triangle Park, and Satellite locations.

Telephone devices are a mix of older H.323 only devices such as the 4601, 4610, 4620, 4621, 4690, 1692, 9620L, 9630, 9640, and 9650 devices and H.323/SIP devices such as 9608, 9611G, 9621, 9621G, 9641, and 9641G devices throughout the agency. All devices presently are configured as H.323 devices on the network as noted in Section J.3.1.4 Site Telephone Inventory.

System programming is performed locally through the EPA network to the System Manager or remotely through the Avaya Secure Access Link (SAL) infrastructure with Policy Server. Additionally, SAL monitors all system platform hardware and notifies the EVS contractor's NOC in the event of any minor or major alarms.

C.7 Technical Requirements

The Contractor's services shall meet the requirements described in the referenced section for the service in the *EIS Contract*, as well as any custom EPA requirements detailed in this SOW.

The Contractor shall engineer, design, configure, provide, and maintain a secure, private, dedicated data communications solution that will simultaneously provide EPA voice, video, and data transmission among all locations listed in attachment J.1 Pricing Workbook.

The Contractor shall provide the services defined in the sub-sections below, in the quantities and locations identified in Section J.1.

C.7.1 Data Services Tasks

C.7.1.1 Virtual Private Network Service (VPNS)

The Contractor's delivered Virtual Private Network Service (VPNS) solution shall meet the requirements described in Section C.2.1.1: Virtual Private Network Service (VPNS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractor's Virtual Private Network Service (VPNS) solution shall replace the IP/MPLS converged managed network solution at the agency presently in place.

The Virtual Private Network Service (VPNS) that is presently in place and that is required to be transitioned is identified in Section J.1: Pricing Workbook. Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.1.1.1 Connectivity

The Contractor's solution shall meet the connectivity requirements as described in Section C.2.1.1.1.3: Connectivity within the VPNS section in the *EIS Contract*.

The Contractor shall provide secure MPLS-enabled IP VPNS Intranet, Extranet and Remote Access solution for the agency networks.

The Contractor's VPNS solution shall provide any-to-any connectivity facilitating the creation of fully or partially meshed networks between node devices across the Contractor's IP backbone.

C.7.1.1.2 Standards

The Contractor's solution shall meet the standards requirements as described in Section C.2.1.1.1.2 Standards within the VPNS section in the *EIS Contract*.

C.7.1.1.3 Technical Capabilities

The Contractor's solution shall meet the connectivity requirements as described in Section C.2.1.1.1.4: Technical Capabilities within the VPNS section in the *EIS Contract*.

The Contractor shall provide engineering designs and configurations to implement VPNS at each of the agency's locations. With EPA's approval, the Contractor shall implement its solution.

Additionally, the Contractor's VPNS solution shall provide:

- Segregation of traffic
- Multicasting
- High availability
- Scalability
- Class of service capabilities
- Agnostic access arrangement compatibility
- Secure and reliable transport of packets
- Edge to edge encryption

The Contractor's VPNS solution shall be capable of supporting a range of applications such as Voice over IP, IP video and video-teleconferencing, IP-based mainframe and database transactions, and other bulk IP data transfer services.

The Contractor's VPNS solution shall be capable of scaling to meet the traffic volumes and Class of Service (COS) policies necessary to carry various types of traffic, in satisfaction of the needs of all the agency applications.

The Contractor's VPNS solution shall be logically or physically separate from all other of the Contractor's customer's traffic, such as that provided by an MPLS network with dynamic VPNs.

The Contractor shall restrict the agency's routing tables and other network information to only authorized, cleared personnel.

C.7.1.1.4 Features

The Contractor's solution shall meet the connectivity requirements as described in Section C.2.1.1.2: Features within the VPNS section in the *EIS Contract*.

All capabilities described in this section and the delivered designs shall preserve the security functions and integrity of the network as described in this SOW and the requirements of the *EIS Contract*.

C.7.1.1.5 Interfaces

The Contractor's solution shall meet the interface requirements as described in Section C.2.1.1.3: Interfaces within the VPNS section in the *EIS Contract*.

C.7.1.1.6 Performance Metrics

The Contractor's delivered Virtual Private Network Service (VPNS) solution shall meet the performance levels as specified in the *EIS Contract* in C.2.1.1.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs.

C.7.1.1.7 VPNS Special Requirements

C.7.1.1.7.1 Remote Access / Optional

EPA is considering two different options for remote access service under the GSA *EIS Contract*. The two options are: 1) a Premise-based Remote Access System (see C.7.1.1.7.1) or 2) a Remote Access Service through the MTIPS (see C.8.2.8.1). The Contractors shall deliver solutions to both options. EPA will optionally elect to order one of these options for remote access.

The Contractor's delivered Premise-Based Remote Access System shall:

- Support 12,500 concurrent remote users, with the capability to expand to 20,000 concurrent remote users
- Be implemented at two separate EPA locations:
 - Potomac Yard Data Center located in Arlington, Virginia
 - NCC located in Research Triangle Park, North Carolina
- Maintain access to TIC portals

- Each TIC portal shall support 12,500 concurrent remote users with the capability to expand to 20,000 concurrent remote users.
- All remote access requirements pertain to EPA GFE will include GFE laptops, GFE I Pads, and GFE I Phones. Non GFE remote access requirements are handled through VDI

The Contractor's delivered Premise-Based Remote Access System shall include a test server for dedicated agency use for the purpose of:

- creating agency specific policies
- testing policies
- certifying configurations
- implementing agency profiles into the production environment
- mimicking the configurations to stage agencies in a pre-production environment

The Contractor's delivered Premise-Based Remote Access System shall include access to and use of the Contractor's:

- software modules,
- Remote Access Service NOC for management, support and monitoring capabilities
- Service Management Console

The Contractor's Premise-Based Remote Access System shall include Contractor 24x7x365 telephone and email support, along with management, monitoring and availability reporting of the Remote Access System.

C.7.1.1.7.2 Direct Cloud Interconnect

EPA requires VPNS access to commercial Cloud Service Providers (CSPs) such as Amazon Web Services (AWS) and Microsoft Azure. Currently this is an AT&T NetBond service. The Contractor shall include the IP transport portion of this service including any bandwidth usage but the CSP portion of the service such as AWS Direct Access or Microsoft Express Route shall not be included which EPA acquires them under a separate contract vehicle.

Any associated MNS or MSS service for this connection shall not be bundled with the connection and instead be proposed under MNS and MSS.

The Section J.1 Pricing Workbook includes the VPNS CSPC CLINs for this service.

C.7.1.2 Ethernet Transport Service (ETS)

The Contractor's Ethernet Transport Service (ETS) solution shall meet the requirements described in Section C.2.1.2: Ethernet Transport Service (ETS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Ethernet Transport Service (ETS) that is presently in place and that is required to be transitioned is identified in Section J.1: Pricing Workbook. Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.1.2.1 Connectivity

The Contractor's solution shall meet the connectivity requirements as described in Section C.2.1.2.1.3: Connectivity within the ETS section in the *EIS Contract*.

C.7.1.2.2 Standards

The Contractor's solution shall meet the standards requirements as described in Section C.2.1.2.1.2: Standards within the ETS section in the *EIS Contract*.

C.7.1.2.3 Technical Capabilities

The Contractor's solution shall meet the technical capabilities as described in Section C.2.1.2.1.4, Technical Capabilities within the ETS section in the *EIS Contract*.

C.7.1.2.4 Features

There are no features described in the ETS section of the *EIS Contract*.

C.7.1.2.5 Interfaces

The Contractor's solution shall meet the interface requirements as described in Section C.2.1.2.3, Interfaces within the ETS section in the *EIS Contract*.

C.7.1.2.6 Performance Metrics

The Contractor's Ethernet Transport Service (ETS) solution shall meet the performance levels as specified in the *EIS Contract* in Section C.2.1.2.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs. The Contractor's Ethernet Transport Service (ETS) solution shall meet the performance levels and AQL of KPIs for Ethernet Transport Service (ETS).

C.7.1.3 Private Line Service (PLS)

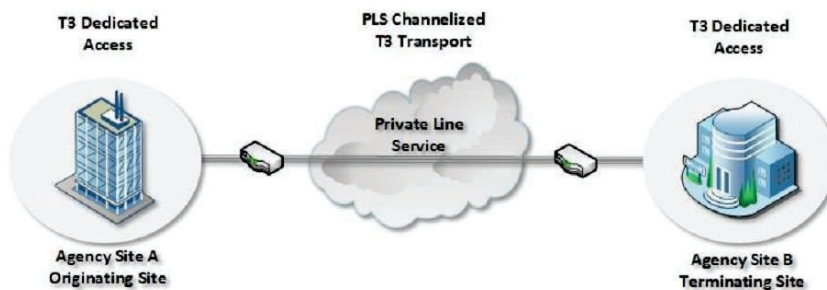
The Contractor's Private Line Service (PLS) solution shall meet the requirements described in Section C.2.1.4: Private Line Service of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Private Line Service (PLS) that is presently in place and that is required to be transitioned is identified in Section J.1: Pricing Workbook. Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.1.3.1 Connectivity

The Contractor's Private Line Service (PLS) solution shall meet the connectivity requirements as described in Section C.2.1.4.1.3: Connectivity within the ETS section in the *EIS Contract* and depicted in Figure 6 Private Line Service.

Figure 6 Private Line Service



C.7.1.3.2 Standards

The Contractor's Private Line Service (PLS) solution shall comply with the following standards as described in Section C.2.1.4.1.2: Standards within the PLS section of the *EIS Contract*.

C.7.1.3.3 Technical Capabilities

The Contractor's Private Line Service (PLS) solution shall provide the following technical capabilities as described in Section C.2.1.4.1.4: Technical Capabilities within the PLS section of the *EIS Contract*. All capabilities are mandatory unless marked as optional.

C.7.1.3.4 Features

The Contractor's Private Line Service (PLS) solution shall include all features as described in Section C.2.1.4.2: Features within the PLS section of the *EIS Contract*.

C.7.1.3.5 Interfaces

The Contractor's Private Line Service (PLS) solution shall include all interfaces as described in Section C.2.1.4.3: Interfaces within the PLS section of the *EIS Contract*.

C.7.1.3.6 Performance Metrics

The Contractor's Private Line Service (PLS) solution shall meet the performance levels as specified in the *EIS Contract* in PLS C.2.1.4.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs. The Contractor's Private Line Service (PLS) solution shall meet the performance levels and AQL of KPIs for Private Line Service (PLS).

C.7.1.4 Internet Protocol Service (IPS)

The Contractor's Internet Protocol Service (IPS) solution shall meet the requirements described in Section C.2.1.7 Internet Protocol Service (IPS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

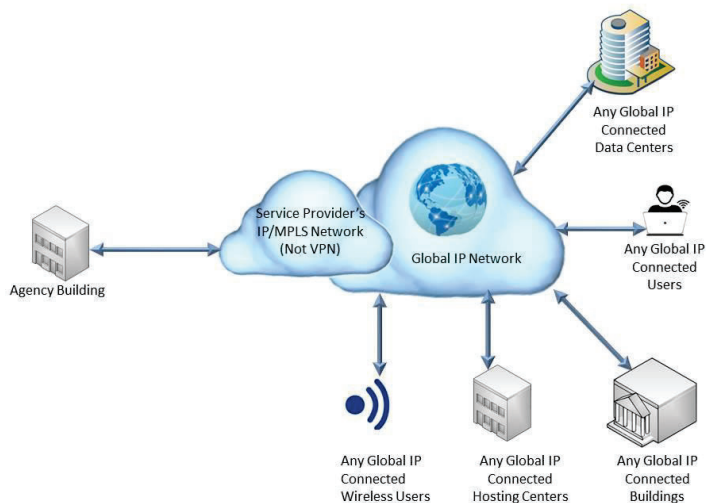
The Contractor shall provide a like-for-like technology for the migration of Internet Protocol Service (IPS) circuits to the GSA *EIS Contract*.

The Internet Protocol Service (IPS) that is presently in place and that is required to be transitioned is identified in Section J.1: Pricing Workbook. Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.1.4.1 Connectivity

The Contractor's solution shall meet the connectivity requirements as described in Section C.2.1.7.1.3: Connectivity within the IPS section in the *EIS Contract* and depicted in Figure 7 below.

Figure 7. Internet Protocol Service Interfaces Depiction



C.7.1.4.2 Standards

The Contractor's solution shall meet the standards requirements as described in Section C.2.1.7.1.2: Standards within the IPS section in the *EIS Contract*.

C.7.1.4.3 Technical Capabilities

The Contractor's solution shall meet the technical capability requirements as described in Section C.2.1.7.1.4: Technical Capabilities within the IPS section in the *EIS Contract*.

C.7.1.4.4 Features

The Contractor's solution shall meet the technical capability requirements as described in Section C.2.1.7.2: Features within the IPS section in the *EIS Contract*.

C.7.1.4.5 Interfaces

The Contractor's solution shall meet the interface requirements as described in Section C.2.1.7.3: Interfaces within the IPS section in the *EIS Contract*.

C.7.1.4.6 Performance Metrics

The Contractor's Internet Protocol Service (IPS) solution shall meet the performance levels as specified in the *EIS Contract* in Section C.2.1.7.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs. The Contractor's Internet Protocol Service (IPS) solution shall meet the performance levels and AQL of KPIs for Internet Protocol Service (IPS).

C.7.2 Voice Services Tasks

C.7.2.1 Internet Protocol Voice Service (IPVS)

The Contractor's Internet Protocol Voice Services (IPVS) solution shall meet the requirements described in Section C.2.2.1 Internet Protocol Voice Service (IPVS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Agency desires to transition to the Internet Protocol Voice Service (IPVS) hosted solution as soon as possible after award of the *EIS Contract*. The Agency's Enterprise Voice Services (EVS) contract expires in May of 2021 with the possibility of extending the Enterprise Voice Services (EVS) contract for a period of four months until September of 2021. The Agency is requiring as an option the Voice Managed Network Services (VMNS) solution as described in C.7.3.1.7.2., if the transition extends past the September 2021 timeframe, to continue to support the Avaya infrastructure provided under the Enterprise Voice Services (EVS) contract for the existing users.

The Contractor shall provide as part of the Transition Plan, the timeline of the transition of telephone users by site to the Internet Protocol Voice Service (IPVS) solution. After successful transition to the Internet Protocol Voice Service (IPVS) solution, the Agency will terminate the Voice Managed Network Services (VMNS) for that site and disconnect any CSVS PRI's or CSVS Analog Lines at that site that had previously been providing PSTN access. The Contractor shall include in their proposals the two options listed below for transitioning the EPA

voice services to EIS. The agency will choose to implement the option(s) that best meets the needs of the agency.

The Contractors shall provide the following solutions that meet the needs of the agency:

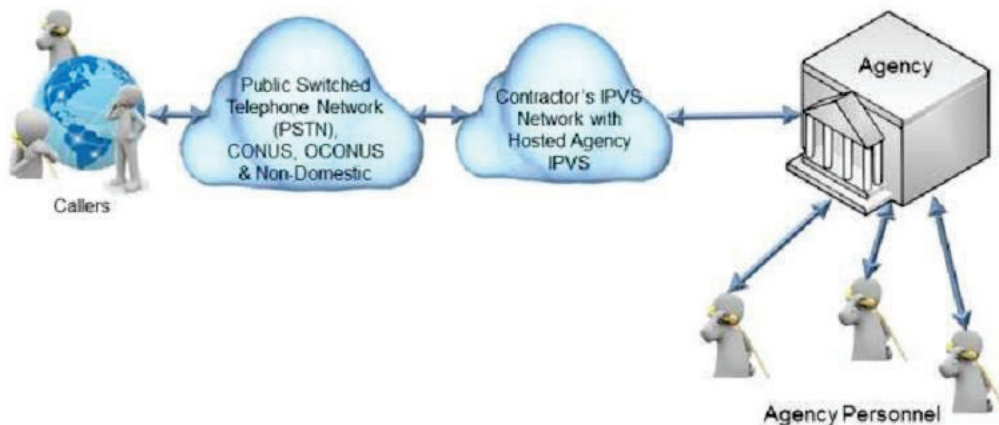
1. IPVS Hosted solution that will meet the requirements as stated in GSA EIS Section C, paragraph C.2.2.1.4. Performance Metrics.
2. Voice Managed Network Services (VMNS) solution as described in C.7.3.1.7.2.

The agency also requires, as options, other IPVS services such as Managed LAN Service in Section C.7.2.1.7 in conjunction with the hosted IPVS or Session Initiation Protocol (SIP) Trunk Service in Section C.7.2.1.8 as an interim solution during the transition.

C.7.2.1.1 Connectivity

The Contractor's solution shall meet the connectivity requirements as described in Section C.2.2.1.1.3: Connectivity, within the IPVS section in the *EIS Contract* and depicted in Figure 8 below.

Figure 8 Internet Protocol Voice Service Depiction



C.7.2.1.2 Standards

The Contractor's solution shall meet the standards requirements as described in Section C.2.2.1.1.2: Standards, within the IPVS section in the *EIS Contract*.

C.7.2.1.3 Technical Capabilities

The Contractor's solution shall meet the technical capabilities requirements as described in Section C.2.2.1.1.4: Technical Capabilities, within the IPVS section in the *EIS Contract*.

The EIS Contractor shall plan, design, test, implement, and deploy the Internet Protocol Voice Services (IPVS) capability and features, including the underlying services for connectivity and access, to meet the agency's requirements for voice over the agency's managed IP network.

The Contractor's solution shall provide for interoperability between the Contractor's IP-based network and the PSTN, and with agency UNI requirements as described in Section C.7.2.1.3.2.

The Contractor's solution shall separate voice and data traffic, as referenced in NIST Special Publication 800-58. The Contractor shall describe how it plans to meet this requirement for separating voice and data traffic in the network.

The *EIS Contractor's* response shall identify the proposed codecs on the WAN and LAN for the voice solution.

The Contractor's solution shall comply with emergency service requirements, including 911 and E911 services, and identify the location of originating stations and route them to the appropriate Public Safety Answering Point (PSAP). The Contractor's solution shall address Kari's law and how the Contractor intends to meet the requirements of the law.

The Contractor's IPVS hosted solution shall include capability for integrating local survivability and limited secondary PSTN access, or possibly broadband access services, to deliver a highly available solution.

The Contractor's solution shall include training the agency system administration staff in the maintenance, administration and operation of the Internet Protocol Voice Services (IPVS) system.

The Contractors shall state in their solution how requests for call detail records and electronic copies of voice mail messages are handled for the agency's customers, in the case of legal proceedings, investigations, inquiries, or other agency needs.

C.7.2.1.3.1 IPVS Locations

Table 6: IPVS includes the facility name, address, city, state, and zip code for each location. The agency serves approximately 23,000 H.323/SIP endpoints and 5,000 traditional analog/ISDN BRI endpoints across the locations identified.

Table 6: IPVS Locations

Summary Telecom Inventory				
Facility Name	Street Address	City	State	Zip
HQ				
One Potomac Yard	2777 Crystal Drive	Arlington	VA	22202
Ardwick Industrial Plaza	8335 - 8361 Ardmore Ardwick	Landover	MD	20785-1622
Ariel Rios Federal Building	1200 Pennsylvania Ave., NW	Washington	DC	20460
EPA East/EPA West /Connecting Wing	1201-1301 Constitution Avenue, NW	Washington	DC	20004
Mount Weather	19844 Blue Ridge Mountain Road	Mount Weather	VA	20135
Emergency Operations Center	1200 Pennsylvania Ave., NW (5104A)	Washington	DC	20005-3105
REGION 1				
John W. McCormack Federal Building	5 Post Office Square, Suite 100	Boston	MA	2109-3912
New England Regional Lab	11 Technology Drive	Chelmsford	MA	08163-2431
Edison Laboratory	2890 Woodbridge Avenue	Edison	NJ	08837-3679
REGION 2				
Ted Weiss Federal Office Building	290 Broadway	New York	NY	10007-1866
Caribbean Environmental Protection Division	Centro Europa Building #417, 1492 Ponce de Leon Avenue, Stop 22	Santurce	PR	00907-4012
REGION 3				
Annapolis City Marina	410 Severn Avenue	Annapolis	MD	21403-2517

Emergency Operations, Conference & Training Center	707 Chelsea Parkway	Boothwyn	PA	19061
Environmental Science Center	701 Mapes Road	Ft. Meade	MD	20755-5350
Region 3 Headquarters	1650 Arch Street	Philadelphia	PA	19103-2029
Wheeling Field Office	1060 Chaline Street, Suite 303	Wheeling	WV	26003-2927
REGION 4				
Sam Nunn Atlanta Federal Center	61 Forsyth Street, SW	Atlanta	GA	30303-8701
Gulfport	2510 14th Street, 12th Floor, Hancock Building	Gulfport	MS	39501
RTP				
Human Studies Facility	104 Mason Farm Road	Chapel Hill	NC	27514
RTP - Laboratory & Office Building	109 TW Alexander Drive	RTP	NC	27711
RTP - National Computer Center alias RTP Host System	109 TW Alexander Drive, Room N238	RTP	NC	27711
Grand Slam Buildings	Page Road & I40	RTP	NC	27514
REGION 5				
Ralph H. Metcalfe Federal Building	77 West Jackson Boulevard	Chicago	IL	60604-3511
Federal Building	536 South Clark Street	Chicago	IL	60605-1509
Steinmart Plaza	25089 Center Ridge Road	Westlake	OH	44145-4114
Willowbrook Center	600 Joliet Road	Willowbrook	IL	60527-5633
Cincinnati				
Andrew W. Breidenbach Environmental Research Center	26 W. Martin Luther King Drive	Cincinnati	OH	45268
Test and Evaluation Facility	1600 Gest Street	Cincinnati	OH	45204-2022
Center Hill Research Facility	5995 Center Hill Avenue	Cincinnati	OH	45224-1701

Experimental Stream Facility	1003 U.S. Highway 50	Milford	OH	45150
Erlanger	4900 Olympic Blvd	Erlanger	KY	41018
REGION 6				
Fountain Place	1445 Ross Avenue	Dallas	TX	75202-2812
Pioneer Building	4050 Rio Bravo	El Paso	TX	79902-1061
Environmental Laboratory	10625 Fallstone Road	Houston	TX	77099
Addison	16650 Westgrove Road	Addison	TX	75202
REGION 7				
Region 7 Headquarters	11201 Renner Boulevard	Lenexa	KS	66219
Kansas City Science & Technology Center	3rd & Minnesota Avenues	Kansas City	KS	66101-2912
Hunt Midwest, Subtrop Building 81C	8600 NE Underground Road, Pillar 253	Kansas City	MO	64161
REGION 8				
Region 8 Headquarters	1595 Wynkoop Street	Denver	CO	80202
Denver Host System	1595 Wynkoop Street	Denver	CO	80202
Region 8 Montana Office	10 W 15th Street, Suite 3200	Helena	MT	59626
National Enforcement Investigations Center	Denver Federal Center, West 6th Avenue & Kipling Street	Lakewood	CO	80225-0000
REGION 9				
Central Regional Laboratory	1337 South 46th Street, Bldg 201	Richmond	CA	94804-4698
610 West Ash Street	610 West Ash Street	San Diego	CA	92101-3300
75 Hawthorne Street	75 Hawthorne Street	San Francisco	CA	94105-3920
Rapid Response Center Warehouse	674 Harrison Street	San Francisco	CA	94105-3917

So Cal Field Office	600 Wilshire Boulevard	Los Angeles	CA	90017
Region 9 Pacific Islands Contact Office	300 Ala Moana Boulevard, Rm 5124	Honolulu	HI	96850
Rapid Response Center Warehouse	2250 Obispo Avenue, Suite 101	Signal Hill	CA	90755-4026
REGION 10				
ERU Warehouse	5761 Silverado Way, Lot 4B	Anchorage	AK	99518
Alaska Operations Office	222 West 7th Avenue	Anchorage	AK	99513-7500
Idaho Operations Office	1455 North Orchard	Boise	ID	83706-2239
Coeur D' Alene Office	1910 Northwest Boulevard, Suite 208	Coeur D' Alene	ID	83814-2676
Washington Operations Office	300 Desmond Drive, SE	Lacey	WA	98503-1274
Manchester Regional Laboratory	7411 Beach Drive East	Port Orchard	WA	98366
Oregon Operations Office	805 SW Broadway	Portland	OR	97205
Hanford Project Office	309 Bradley Landing, Suite 115	Richland	WA	99352
Seattle Emergency Response Unit Warehouse	1620 South 92nd Place, Suite B	Seattle	WA	98108
Park Place Building	1200 Sixth Avenue	Seattle	WA	98101-3123
CID				
Islander Park 1 Building	7550 Lucerne Drive	Middleburg Heights	OH	44130-6588
GT Mickey Leland Federal Building	1919 Smith Street	Houston	TX	77002-8049
OAR				
National Air and Radiation Environmental Laboratory	Maxwell AFB, Gunter Annex, 540 South Morris Avenue	Montgomery	AL	36115-2601
National Vehicle Fuel & Emissions Laboratory	2565 Plymouth Road	Ann Arbor	MI	48105

NVFEL Office Building	2000 Traverwood Drive	Ann Arbor	MI	48105-2195
La Plaza Buildings	4220 Maryland Parkway	Las Vegas	NV	89119-7533
ORD				
Environmental Effects Research Laboratory	27 Tarzwell Drive	Narragansett	RI	02882
Science and Ecosystems Support Division Laboratory	980 College Station Road	Athens	GA	30605-2720
Region 4 Field Equipment Center, The Paul Martin Building	396 Commerce Boulevard	Athens	GA	30622-2224
Ecosystems Research Division	960 College Station Road	Athens	GA	30605-2700
Lifespan Center	960 College Station Road	Athens	GA	30605-2700
Field Research Annex	625 Bailey Road	Athens	GA	30605-1827
Gulf Ecology Division	One Sabine Island Drive	Gulf Breeze	FL	32561-5299
Large Lakes & Rivers Forecasting Research Station	9311 Groh Road	Grosse Ile	MI	48138-1697
Duluth Laboratory	Edgshore Park Subdivision, Outlet D	Duluth	MN	55804
Robert S. Kerr Environmental Research Lab	P.O. Box 1198, 919 Kerr Research Drive	Ada	OK	74820
Gaar Corner	P.O. Box 1198, 919 Kerr Research Drive	Ada	OK	74820
UNLV On-Campus EPA Facilities	944 East Harmon	Las Vegas	NV	89119-6748
Western Ecology Division	200 SW 35th Street	Corvallis	OR	97333-4902
WED Jefferson Street Building	3731 SW Jefferson Way	Corvallis	OR	97333-3971
Willamette Research Station	1350 SE Goodnight Road	Corvallis	OR	97333-2104
Pacific Coastal Ecology Branch	2111 SE Marine Science Drive	Newport	OR	97365

C.7.2.1.3.2 User Network Interfaces

The Contractor's solution shall include the User Network Interface (UNI)'s for the non-proprietary telephony analog station interfaces and non-proprietary telephony ISDN BRI station interfaces as required for each location in Table 7: UNI Requirements.

Table 7: UNI Requirements

UNI Requirements			
Facility Name	Analog Stations	IP Stations	Basic Rate Interface Stations
HQ			
One Potomac Yard	168	1050	0
Ardwick Industrial Plaza	0	8	0
Ariel Rios Federal Building	384	3225	0
EPA East/EPA West /Connecting Wing	360	1745	0
Mount Weather	0	143	0
Emergency Operations Center	0	100	0
REGION 1			
John W. McCormack Federal Building	96	698	8
New England Regional Lab	48	174	8
REGION 2			
Edison Laboratory	72	296	0
Ted Weiss Federal Office Building	72	779	0
Caribbean Environmental Protection Division	0	24	0
REGION 3			
Annapolis City Marina	24	75	8
Emergency Operations, Conference & Training Center	0	10	8
Environmental Science Center	48	120	8
Region 3 Headquarters	216	1176	16
Wheeling Field Office	0	20	8
REGION 4			
Sam Nunn Atlanta Federal Center	144	1126	32
Gulfport	0	50	0
RTP			
Human Studies Facility	24	120	0
RTP - Laboratory & Office Building	312	2204	8
RTP - National Computer Center alias RTP Host System	72	200	8
Grand Slam Buildings	0	15	0
REGION 5			

Ralph H. Metcalfe Federal Building	96	1212	12
Federal Building	0	50	0
Steinmart Plaza	4	25	8
Willowbrook Center	0	20	0
Cincinnati			
Andrew W. Breidenbach Environmental Research Center	216	890	8
Test and Evaluation Facility	48	25	0
Center Hill Research Facility	24	20	0
Experimental Stream Facility	0	20	0
Erlanger	24	100	8
REGION 6			
Fountain Place	96	711	16
Pioneer Building	0	20	0
Environmental Laboratory	96	140	16
Addison	0	100	16
REGION 7			
Region 7 Headquarters	120	545	0
Kansas City Science & Technology Center	52	100	0
Hunt Midwest, Subtrop Building 81C	4	30	8
REGION 8			
Region 8 Headquarters	48	892	0
Denver Host System alias DEN Host System	0	0	0
Region 8 Montana Office	0	100	0
National Enforcement Investigations Center	48	126	0
REGION 9			
Central Regional Laboratory	24	100	0
610 West Ash Street	0	40	0
75 Hawthorne Street	216	891	0
Rapid Response Center Warehouse	0	20	0
So Cal Field Office	24	40	0
Region 9 Pacific Islands Contact Office	0	20	0
Rapid Response Center Warehouse	0	20	0
REGION 10			
ERU Warehouse	4	10	0
Alaska Operations Office	4	20	0
Idaho Operations Office	4	20	0
Coeur D' Alene Office	0	20	0
Washington Operations Office	4	20	0
Manchester Regional Laboratory	4	60	0
Oregon Operations Office	4	20	0
Hanford Project Office	4	20	0
Seattle Emergency Response Unit Warehouse	4	10	0
Park Place Building	24	732	0

CID			
Islander Park 1 Building	4	40	0
GT Mickey Leland Federal Building	0	10	0
OAR			
National Air and Radiation Environmental Laboratory	72	140	16
National Vehicle Fuel & Emissions Laboratory	288	150	16
NVFEL Office Building	0	160	0
ORD			
La Plaza Buildings	96	120	16
Environmental Effects Research Laboratory	48	100	0
Science and Ecosystems Support Division Laboratory	24	118	0
Region 4 Field Equipment Center, The Paul Martin Building	0	40	0
Ecosystems Research Division	96	240	8
Lifespan Center	0	20	0
Field Research Annex	0	20	0
Gulf Ecology Division	72	120	0
Large Lakes & Rivers Forecasting Research Station	24	100	8
Duluth Laboratory	192	160	0
Robert S. Kerr Environmental Research Lab	96	100	0
Gaar Corner	0	20	0
UNLV On-Campus EPA Facilities	96	100	0
Western Ecology Division	48	100	0
WED Jefferson Street Building	48	100	0
Willamette Research Station	24	80	0
Pacific Coastal Ecology Branch	24	80	0

C.7.2.1.3.3 Telephone Inventory

EPA currently supports a variety of handsets on the network that are a mix of older H.323 only devices such as the Avaya 4601, Avaya 4610, Avaya 4620, Avaya 4621, Avaya 4690, and Avaya 1692 IP Telephone devices and H.323/SIP devices such as the Avaya 9620L, Avaya 9630, Avaya 9640, and Avaya 9650, Avaya 9608, Avaya 9611G, Avaya 9621, Avaya 9621G, Avaya 9641, and Avaya 9641G IP Telephone devices. All IP Telephone devices are presently configured as H.323 devices on the network.

All IP Telephone devices have reached the end of support from the manufacturer and shall be replaced by the Contractor. The Contractor shall furnish and install the IP Telephone devices in the type and quantities included in Table 8: IP Telephone Breakdown. Analog 2500 type telephones still exist to serve locations with adverse conditions, areas with no network

connections, and critical service locations. These analog 2500 type telephones will be not be replaced during the transition. Secure Terminal Equipment (STE) is used in conjunction with the Basic Rate Interface Lines and will not be replaced during the transition. The Contractor's IPVS solution shall interoperate with the EPA's existing analog 2500 telephones and Secure Terminal Equipment (STE).

Table 8: IP Telephone Breakdown

IP Telephone Breakdown	
Quantity	Item Description
1133	Single Line IP Telephone / 5% of 22656 IP Telephone Devices
18124	Basic Multiline IP Telephone / 80% of 22656 IP Telephone Devices
2266	Enhanced Multiline IP Telephone / 10% of 22656 IP Telephone Devices
1133	Teleconference IP Telephone / 5% of 22656 IP Telephone Devices

The tables below list the features and characteristics for each IP Telephone Device; Table 9 Single Line IP Telephones, Table 10 Basic Multiline IP Telephones, Table 11 Enhanced Multiline IP Telephones, and Table 12 Teleconference IP Telephones, and as identified above in Table 8, IP Telephone Breakdown.

Table 9 Single Line IP Telephone

Single Line IP Telephone	
Feature	Characteristics
Applications	Lobbies, Waiting Areas, Lunch Rooms, Manufacturing Areas, Labs, and Hallways
Audio	Opus Codec, G.711 a/u, G.722, G.726A, G.729A, and G.729AB
Call Handling	SIP, Hold, Transfer, TLS/SRTP for Encryption Support, Desk or Wall Mounted, and Hearing Aid Compatible Headset
User Interface	Single Line, Three Soft Keys, and Status Indicators
Connections	Dual 10/100 Ethernet ports to support co-located PC
Power Requirements	Power over Ethernet (PoE) 802.3af as a Class 1 device

Table 10 Basic Multiline IP Telephone

Basic Multiline IP Telephone	
Feature	Characteristics
Applications	Basic Voice Communication Device for Users
Audio	Opus Codec, G.711 a/u, G.722, G.726A, G.729A, and G.729AB
Call Handling	SIP, Full Duplex Speakerphone, Message Waiting Indicator, Speakerphone, Mute, Hold, Transfer, TLS/SRTP for Encryption Support, Headset Capable, and Hearing Aid Compatible Headset
User Interface	Four Lines, Four Soft Keys, Display, and Status Indicators
Connections	Dual 10/100/1000 Gigabit Ethernet ports to support co-located PC
Power Requirements	Power over Ethernet (PoE) 802.3af as a Class 1 device

Table 11 Enhanced Multiline IP Telephone

Enhanced Multiline IP Telephone	
Feature	Characteristics
Applications	Enhanced Voice Communication Device for Users
Audio	Opus Codec, G.711 a/u, G.722, G.726A, G.729A, and G.729AB
Call Handling	SIP, Full Duplex Speakerphone, Message Waiting Indicator, Speakerphone, Mute, Hold, Transfer, TLS/SRTP for Encryption Support, Headset Capable, Bluetooth Capable, and Hearing Aid Compatible Headset
User Interface	Eight Lines, Four Soft Keys, Display, and Status Indicators
Connections	Dual 10/100/1000 Gigabit Ethernet ports to support co-located PC
Power Requirements	Power over Ethernet (PoE) 802.3af as a Class 1 device

Table 12 Teleconference IP Telephone

Conference IP Telephone	
Feature	Characteristics
Applications	Conference Rooms
Audio	G.711
Call Handling	SIP, Hold, TLS/SRTP for Encryption Support, Desk Mounted, Omnidirectional Microphone, Pick-Up Range Up to 320 sq ft, Volume Max 90 dB SPL 0.5 m, Capable of Optional Expansion Microphones
User Interface	Single Line, Soft Keys, and Status Indicators
Connections	Ethernet RJ45
Power Requirements	Power over Ethernet (PoE) 802.3af as a Class 3 device

C.7.2.1.4 Features

The Contractor's solution shall include the features that are assignable on a per IP Telephone device basis through system administration and as described in Section C.2.2.1.2, within the IPVS section in the *EIS Contract*. Voice Mail Boxes will be assigned on a per IP Telephone device basis.

C.7.2.1.5 Interfaces

The Contractor's service shall include the interfaces as described in Section C.2.2.1.3: Interfaces within the Internet Protocol Voice Services (IPVS) section of the *EIS Contract*.

C.7.2.1.6 Performance Metrics

The Contractor's IPVS solution shall meet the performance levels as specified in the *EIS Contract* in Internet Protocol Voice Services (IPVS), Section C.2.2.1.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs.

C.7.2.1.7 Managed LAN Service / Optional

The Contractor's Managed LAN Service shall meet the requirements described in Section C.2.2.1.5: Managed LAN Service of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.2.1.8 Session Initiation Protocol (SIP) Trunk Service / Optional

The Contractor's Session Initiation Protocol (SIP) Trunk Service shall meet the requirements described in Section C.2.2.1.6: Session Initiation Protocol (SIP) Trunk Service of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.2.1.8.1 Technical Capabilities and Features

The Contractor's solution shall meet the technical capabilities requirements and features as described in Section C.2.2.1.6.1: Technical Capabilities and Section C.2.2.1.6.2: Features, within the Session Initiation Protocol (SIP) Trunk Service section in the *EIS Contract*.

C.7.2.2 Circuit Switched Voice Service (CSVS)

The Contractor's Circuit Switched Voice Service (CSVS) solution shall meet the requirements as described in Section C.2.2.2: Circuit Switched Voice Service of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

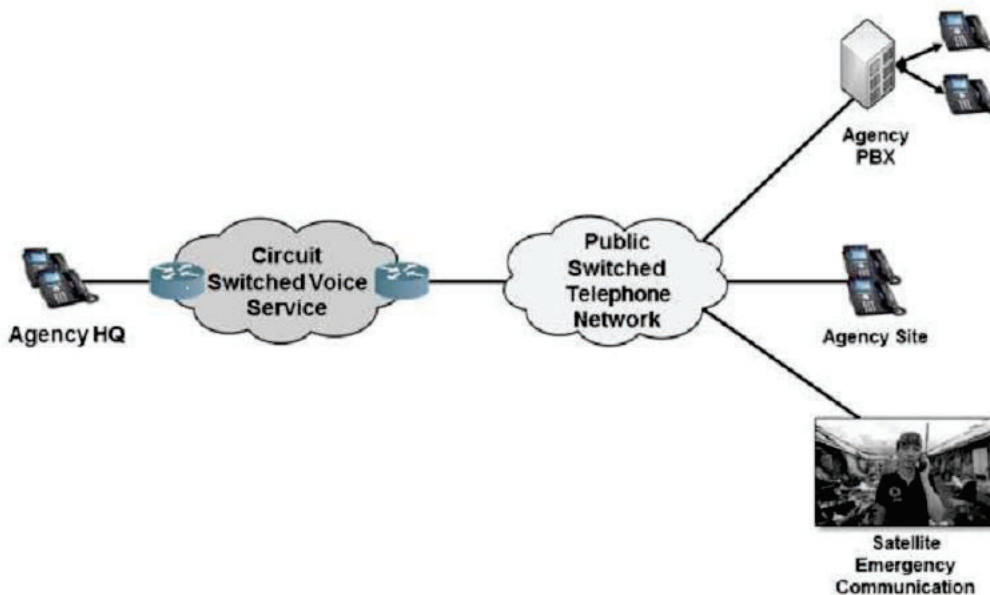
The Contractor shall provide a like-for-like technology for the migration of these Circuit Switched Voice Service (CSVS) circuits to the GSA *EIS Contract*.

The Circuit Switched Voice Service (CSVS) that is presently in place and that is required to be transitioned is identified in Section J.1: Pricing Workbook. Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.2.2.1 Connectivity

The Contractor's Circuit Switched Voice Service (CSVS) solution offering shall meet the connectivity requirements as described in C.2.2.2.1.3: Connectivity within the Circuit Switched Voice Service (CSVS) section in the GSA *EIS Contract* and as depicted below.

Figure 9 Circuit Switched Voice Circuit Depiction



C.7.2.2.2 Standards

The Contractor's Circuit Switched Voice Service (CSV) solution shall include the technical capabilities as described in C.2.2.2.1.2: Standards within the Circuit Switched Voice Service (CSV).

C.7.2.2.3 Technical Capabilities

The Contractor's Circuit Switched Voice Service (CSV) solution offering shall include the technical capabilities as described in C.2.2.2.1.4: Technical Capabilities within the Circuit Switched Voice Service (CSV).

The Contractor's Circuit Switched Voice Service (CSV) solution shall:

- fully comply with emergency service requirements, including 911 and E911 services
- identify the locations of originating stations and route them to the appropriate Public Safety Answering Point (PSAP)
- comply with the new e911 rule called Kari's Law. The Contractor shall explain how the Contractor's Circuit Switched Voice Service (CSV) solution will meet the requirements of this law.

C.7.2.2.4 Features

The Contractor's solution shall include the features as described in C.2.2.2.2 Features within the Circuit Switched Voice Service (CSV) section of the *EIS Contract* and in Table 10 Circuit Switched Voice Services Features.

The Contractor shall include all necessary service-related equipment (SRE), including terminal devices, hardware and software, on the appropriate Circuit Switched Voice Service (CSVs) service and feature CLINs.

C.7.2.2.5 Interfaces

The Contractor's solution shall include the interfaces as described in C.2.2.2.3 Interfaces within the Circuit Switched Voice Service (CSVs) section of the *EIS Contract*.

C.7.2.2.6 Performance Metrics

The Contractor's Circuit Switched Voice Service (CSVs) solution shall meet the performance levels as specified in the *EIS Contract* in CSVs C.2.2.2.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs. The Contractor's Circuit Switched Voice Service (CSVs) solution shall meet performance levels and AQL of KPIs for Circuit Switched Voice Service (CSVs).

C.7.2.2.7 CSVs Special Requirements

C.7.2.2.7.1 Unlimited Local Calling Plan

The Contractor's Circuit Switched Voice Service (CSVs) solution shall provide a local unlimited calling plan that includes at a minimum:

- a local phone number (includes porting of the current number, if required),
- dial tone,
- an unlimited local calling plan,
- allow Long Distance calling on a usage basis, utilizing Dedicated Access,
- blocking of Non-Domestic calling.

C.7.2.3 Toll Free Service (TFS)

The Contractor's Toll-Free Service (TFS) solution shall meet the requirements described in C.2.2.3 Toll-Free Service (TFS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractor shall provide a like-for-like technology for the migration of these Toll-Free Services (TFS) to the GSA *EIS Contract*.

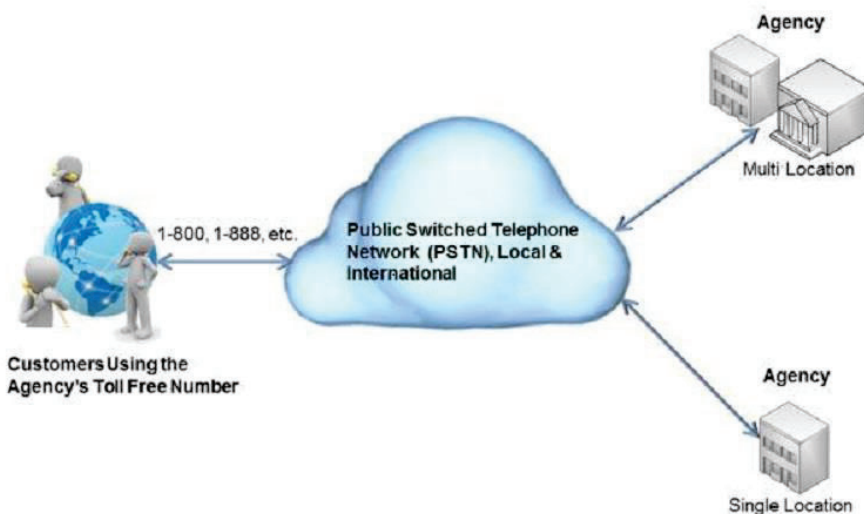
The Toll-Free Service (TFS) that is presently in place and that is required to be transitioned is identified in Section J.1 Pricing Workbook. Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.2.3.1 Connectivity

The Contractor's solution shall meet the connectivity requirements as described in C.2.2.3.1.3: Connectivity within the Toll-Free Service (TFS) section in the *EIS Contract*.

The Contractor's solution for Toll-Free Service shall connect to and interoperate with the PSTN including both wireline and wireless. It is understood that Toll-Free Service uses underlying Voice Service for connectivity as delineated in Section C.2.2.2.1 in the *EIS Contract*. It is further understood that Toll-Free Service shall be provided for both dedicated and switched terminating access arrangements by the *EIS Contractor*.

Figure 10 Toll Free Service Circuit Depiction



C.7.2.3.2 Standards

The Contractor's solution shall meet the connectivity requirements as described in C.2.2.3.1.2: Standards within the Toll-Free Service (TFS) section in the *EIS Contract*.

C.7.2.3.3 Technical Capabilities

The Contractor's service shall include the technical capabilities as described in C.2.2.3.1.4: Technical Capabilities within the Toll-Free Service (TFS) section of the *EIS Contract*.

To support the agency's Toll-Free Service (TFS), the Contractors shall meet the following requirements:

- U.S. and Canadian callers shall be able to reach the agency using TFS Numbers linked to the agency's existing local telephone number (switched access) or a dedicated nodal circuit.

- Non-domestic callers in other countries shall be able to call using International TFS Numbers, making it easy for global customers to reach and access the agency's customer service centers in the U.S.
- Using TFS inbound, calls shall be routed to agency telephone numbers or agency contact centers to deliver seamless 24-hour, around-the-clock support.

The Contractor shall support number portability and shall be able to transition seamlessly the agency's existing toll-free telephone numbers from a previous contract to EIS with minimal disruption and no interference with the calling public.

The Contractor shall assume management and maintenance of existing TFS accounts for the telephone numbers and locations listed in Section J.3.3 Existing Toll-Free Service Telephone Numbers. Table 11 below lists the agency's average usage for domestic and international toll-free minutes.

Table 11 – Agency Toll Free Service Usage

Domestic Average Number of Minutes	International Average Number of Minutes
142,432 Minutes per month	0 Minutes per month

C.7.2.3.4 Features

The Contractor's solution shall include the features as described in C.2.2.3.2: Features within the Toll-Free Service (TFS) section of the *EIS Contract*.

The Contractor shall include all necessary Service-Related Equipment (SRE), including terminal devices and software, on the appropriate TFS basic service and feature CLINs.

C.7.2.3.4.1 TFS Feature Reports

The Contractor's solution shall include the features in the EIS Contract table within Section C.2.2.3.2.1. These features are described in Section C.2.2.3.2.1 TFS Feature Reports within the Toll-Free Service (TFS) section of the *EIS Contract*.

C.7.2.3.5 Interfaces

The Contractor's solution shall include the interfaces as described in C.2.2.3.3 Interfaces within the Toll-Free Service (TFS) section of the *EIS Contract*.

C.7.2.3.6 Performance Metrics

The Contractor's Toll-Free Service section solution shall meet the performance levels as specified in the *EIS Contract* in TFS C.2.2.3.4 Performance Metrics and Section G.8.2.1, Service Performance SLAs.

C.7.2.4 Circuit Switched Data Service (CSDS)

The Contractor's Circuit Switched Data Service (CSDS) solution shall meet the requirements described in C.2.2.4: Circuit Switched Data Service (CSDS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

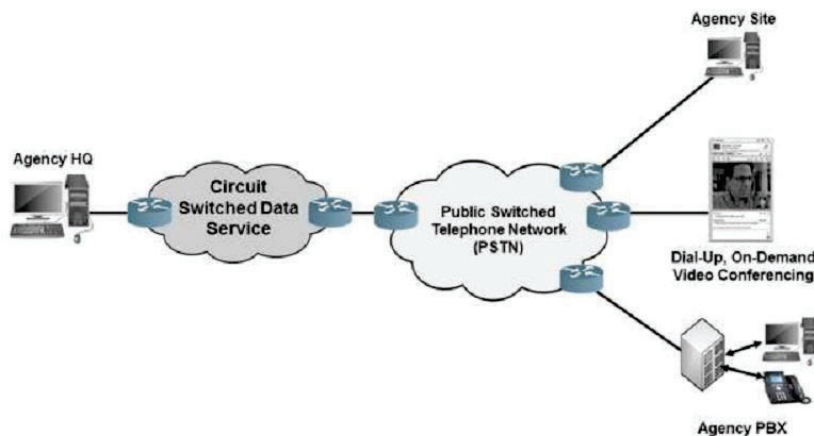
The Contractor shall provide a like-for-like technology for the migration of these CSDS to the GSA *EIS Contract*.

The Circuit Switched Data Service (CSDS) that is presently in place and that is required to be transitioned is identified in Section J.1: Pricing Workbook. Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.2.4.1 Connectivity

The Contractor's Circuit Switched Data Service (CSDS) solution shall meet the requirements described in C.2.2.4.1.3: Connectivity within the Circuit Switched Data Service (CSDS) section in the *EIS Contract* and depicted in Figure 11 below.

Figure 11 Circuit Switched Data Service Depiction



C.7.2.4.2 Standards

The Contractor's Circuit Switched Data Service (CSDS) solution shall meet the requirements described in C.2.2.4.1.2: Connectivity within the Circuit Switched Data Service (CSDS) section in the *EIS Contract*.

C.7.2.4.3 Technical Capabilities

The Contractor's Circuit Switched Data Service (CSDS) solution shall meet the requirements described in Section C.2.2.4.1.4: Technical Capabilities within the Circuit Switched Data Service (CSDS) section in the *EIS Contract*.

C.7.2.4.4 Features

The Contractor's solution shall include the optional features as described in C.2.2.4.2 Features within the Circuit Switched Data Service (CSDS) section of the *EIS Contract* of Dial-In and User-to-User Signaling via ISDN D-Channel.

C.7.2.4.5 Interfaces

The Contractor's solution shall include the mandatory interfaces as described in C.2.2.4.3: Interfaces within the Circuit Switched Data Service (CSDS) section of the *EIS Contract*.

C.7.2.4.6 Performance Metrics

The Contractor's Circuit Switched Data Service section solution shall meet the performance levels as specified in the *EIS Contract* in TFS C.2.2.4.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs.

C.7.3 Managed Services Tasks

C.7.3.1 Managed Network Service (MNS)

The Contractor's Managed Network Service (MNS) solution for agency requirements shall meet the requirements described in C.2.8.1: Managed Network Service (MNS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

As part of this Managed Network Services environment, the agency will continue with a service delivery model upon transition to the GSA *EIS Contract* where separate operational groups are responsible for the ordering, maintenance, and component support of data and voice services for different locations and responsibilities. These operational groups will interact directly with the

EIS Contractor and/or agency internal support team on a day-to-day basis while the agency supports its operational groups in an oversight and assistance role.

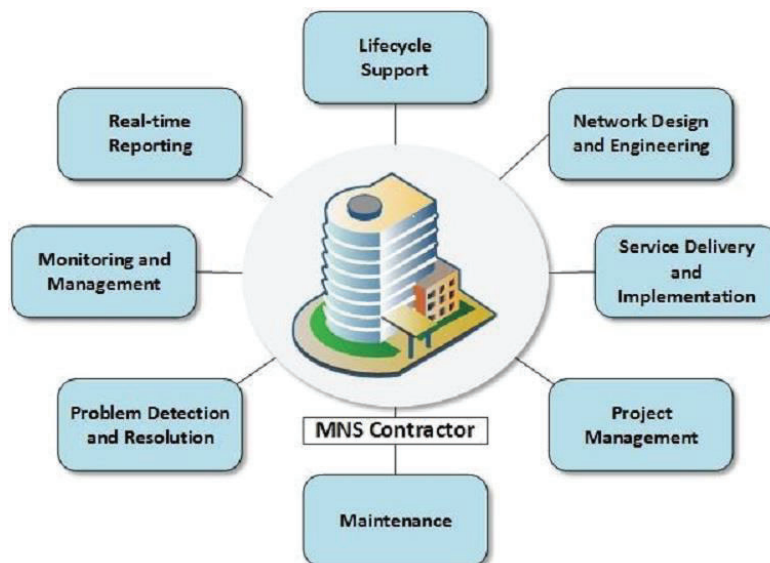
The *EIS Contractor* shall provide a Managed Network Services that is integrated, coordinated and managed in a consistent, coherent, manner delivering the following functions:

- EIS Network Operations Center Operations and Management Systems/Tools
- *EIS Contractor's* Field Support Staff and Systems
- *EIS Contractor* Integrated Local Exchange Carrier (LEC) Support Staff and Systems

The *EIS Contractor* shall allow the agency to leverage the *EIS Contractor's* full range of service delivery processes and platforms for managing - at minimum - the following functions as depicted in Figure 12 Managed Network Services below:

- Lifecycle Support
- Network Engineering and Design
- Service Delivery and Provisioning
- Project Management
- Maintenance
- Problem Detection and Resolution
- Monitoring and Management
- Real-time Reporting

Figure 12 Managed Network Services



The roles and responsibilities of agency and the *EIS Contractor* for the network operations are described at a high level in the table below. The *EIS Contractor* shall work with the agency to refine this relationship by defining operational processes that will optimize the use of agency and *EIS Contractor* resources. It is the agency's expectation that this relationship will evolve over time as the needs of the agency evolve.

Table 12 EPA Enterprise Roles and Responsibilities

EPA Enterprise Roles and Responsibilities		
Functions	EPA Role	<i>EIS Contractor</i> Role
Design and Engineering	Support Role: Review and Approve	Primary Role: Design and Engineering
Transition and Implementation	Support Role: Acceptance and Oversight	Primary Role: Lead and Manage
Monitoring	Oversight	Primary Role: Monitor, tracks, and documents
Trouble Resolution	Oversight	Primary Role: Tier 1, Tier 2, Tier 3, and Tier 4
Trouble Ticketing	Oversight	Primary Role: Ticket Issuance
Configuration Change Management	Review and Oversight	Primary Role: Submission of Change Control Documentation
Performance Management	Review and Oversight	Primary Role: Process, analyze, and report performance information
Reports	Review and Oversight	Primary Role: Produce and analyze
Traffic and Capacity Engineering	Review and Oversight	Primary Role: Analysis, Modeling, and Performance Assessment
Billing	Review and Oversight	Primary Role: Create, Audit, prepare, and Deliver a Bill

C.7.3.1.1 Connectivity

The Contractor's Managed Network Service (MNS) solution shall meet the requirements described in C.2.8.1.1.3: Connectivity within the Managed Network Service (MNS) section in the *EIS Contract*.

C.7.3.1.2 Standards

The Contractor's Managed Network Service (MNS) solution shall meet the requirements described in C.2.8.1.1.2: Standards within the Managed Network Service (MNS) section in the *EIS Contract*.

C.7.3.1.3 Technical Capabilities

The Contractor's proposed Managed Network Service (MNS) solution shall meet the requirements in C.2.8.1.1.4: Technical Capabilities within the Managed Network Service (MNS) section in the *EIS Contract*.

The Contractor shall provide the following MNS capabilities as described in the *EIS Contract* in Section C.2.8.1.1.4.1: Design and Engineering Services and Section C.2.8.1.1.4.2: Implementation, Management, and Maintenance.

Contractors shall allow the agency to perform network scanning of the Contractor-managed devices to satisfy the Homeland Security Continuous Diagnostics and Mitigation (CDM) initiative designed to reduce cybersecurity threats, improve security response capabilities, and streamline FISMA reporting.

The Contractor's MNS solution shall allow the agency to extend READ-WRITE capabilities over managed equipment to select EPA user accounts on a temporary or permanent basis.

The Contractor's MNS solution shall allow access to the following features on managed routers to provide a second layer of network monitoring:

- SNMP READ-ONLY
- Syslog
- SNMP traps

The Contractor shall provide a Customer Portal through a secure, customized web-based interface to allow the agency to manage each service delivery function. The web-based interface shall be accessible through any of the standard Internet browsers used by the agency and its operational groups (i.e., no special client-side software shall be required).

The Contractor shall provide sufficient help desk personnel who will be readily available for real-time discussions to handle inquiries, exceptions, and escalations, although the web-based Customer Portal shall be the first-line vehicle for service delivery.

The Contractor shall provide training to the agency system administration staff in the maintenance, administration, and operation of any MNS services provided.

C.7.3.1.4 Features

The Contractor's Managed Network Service (MNS) solution shall meet the requirements described in C.2.8.1.2: Features within the Managed Network Service (MNS) section in the *EIS Contract*.

C.7.3.1.5 Interfaces

The Contractor's Managed Network Service (MNS) solution shall meet the requirements described in C.2.8.1.3: Interfaces within the Managed Network Service (MNS) section in the *EIS Contract*.

C.7.3.1.6 Special Requirements

C.7.3.1.6.1 Data Managed Network Service (DMNS)

The Contractor shall support the transition of existing MNS services for the agency's data infrastructure from GSA Networkx Contract to the GSA *EIS Contract* as Data Managed Network Services (DMNS) solution, as described in Section C.2.8.1, Managed Network Service of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractor shall provide DMNS as describe herein to all locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

The Data Managed Network Services that the Contractor shall provide shall consist of design and engineering, implementation, management, and maintenance services to support the agency's network enterprise.

The Contractor will be instructed by individual service orders by the agency and shall provide estimates to the agency that contain Service-Related Equipment and Service-Related Labor for guidance, expertise, technical support, and documentation based on the requirements for the individual service order. Details of the instructions and service-related labor requirements for the MNS will be described by the agency in the individual service orders, which may include, but not be limited to, the following;

Contractors shall provide Design and Engineering Services; to include, but not be limited to; Identifying hardware and firmware (e.g., routers, switches, and other SRE), related software, and SRL required by the agency to deliver the EIS services, identifying network components and determining protocols, redundancy, traffic filtering, and traffic prioritization requirements, recommending the appropriate performance levels and network capacities as required, providing complete project management for design, engineering, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation, and coordinating installation activities with the agency to minimize the impact on the current networking environment.

Contractors shall provide implementation, management, and maintenance; access solutions that use a combination of different services (e.g., wireline and wireless access services) for specific agency locations, to meet agency performance metrics for availability and disaster recovery, transport solutions that distribute traffic over multiple Contractor backbone networks to provide redundancy and carrier diversity, and vary the traffic allocation dynamically based on agency performance requirements, customer premises solutions that provide agency-specific interfaces, software, and equipment to meet agency requirements, security solutions as required by the agency, the Contractor shall provide the necessary technical and operational capabilities to ensure the availability and reliability of the agency's network infrastructure and systems, and provides and manages the hardware, firmware and related software required by the agency. Components shall include but are not limited to routers and switches, encryption devices, CSUs/DSUs, hubs, adapters, and modems. As part of the Data Managed Network Service (DMNS) and representative of the requirements in this paragraph, the Contractor shall assume the GFE and the maintenance service for the GFE listed below:

1. Cisco - 2821 w/ AC PWR,2GE,4HWICs,3PVDM,1NME-X,2AIM, IP BASE,64F/256D
2. Cisco - ASR1000-ESP5 - ASR1K Embedded Services Processor,5Gbps, ASR1002 only
3. Cisco - ASR1002 - Cisco ASR1002 Chassis,4 built-in GE, Dual P/S,4GB DRAM
4. Cisco - CISCO2921/K9 - Cisco 2921 w/3 GE,4 EHWIC,3 DSP,1 SM,256MB CF,512MB DRAM, IPB
5. Cisco - CISCO3925/K9 - Cisco 3925 w/SPE100(3GE,4EHWC,4DSP,2SM,256MBCF,1GBDRAM, IPB)
6. Cisco - CISCO3945/K9 - Cisco 3945 w/SPE150(3GE,4EHWC,4DSP,4SM,256MBCF,1GBDRAM, IPB)
7. Cisco - CISCO3945E/K9 - Cisco 3945 w/SPE250,4GE,3EHWC,3DSP
8. Cisco - CISCO3945E-SEC/K9 - Cisco 3945E Security Bundle w/SEC license PAK
9. Cisco - ISR4431/K9 - Cisco ISR 4431 (4GE,3NIM,8G FLASH,4G)
10. Cisco - N9K-C93180YC-EX - Nexus 9300 with 48p 10/25G SFP+ and 6p 100G
11. Cisco - NM-1T3/E3 - One Port T3/E3 Network Module
12. Cisco - PA-POS-10C3 - 1-Port Packet/SONET OC3C/STM1 Port Adapter
13. Cisco - SPA-1X10GE-L-V2 - Cisco 1-Port 10GE LAN-PHY Shared Port Adapter
14. Cisco - SPA-2XOC3-POS - 2-Port OC3 POS Shared Port Adapters
15. Cisco ISR 4331 (3GE,2NIM,1SM,4G FLASH,4G DRAM, IPB)
16. MultiTech Systems - MT5634ZBA-Global-AT&T-NAM - MultiTech 56kbps modem
17. Reelcomm - 9111789-8 - Rack-mountable Code-Operated Switch, 4-Port
18. US Robotics - USR3453C - U.S. Robotics Courier Everything V.92 secure modem

Presently, the agency has the following Service Exceptions to the Data Managed Network Services (MNS) at the following locations of National Computer Center (NCC), William Jefferson Clinton (WJC), Potomac Yard (PYD), Denver, and Chicago and maintains the option to internally manage select locations (i.e. exclude from MNS). As an option, the Contractor shall provide DMNS at those locations identified, if not excluded by the agency.

Contractors shall provide MNS tools to monitor performance of agency-specific networks including transport services, access circuits, and government edge routers, and provide real-time visibility of transport and access services performance. Contractors shall allow the agency to perform network scanning of the Contractors-managed devices to satisfy the Homeland Security Continuous Diagnostics and Mitigation (CDM) initiative designed to reduce cybersecurity threats, improve security response capabilities, and streamline FISMA reporting. Contractors shall provide network management and sustainment support including, but not limited to: manage the network in real-time on a 24x7 basis, support remote management capabilities from the operations center defined in the task order (TO), proactively monitor utilization and performance, probing in intervals of no more than fifteen minutes to ensure proper equipment/network operations, assess and report access and transport services performance and SLAs, assess and report on agency-specific network capacity and performance, and address agency-specific network capacity and performance issues.

Contractors shall provide Managed Network Service to the agency, as applicable, via SNMP read-access data feeds.

Contractors shall provide configuration management tasks and activities, which include, but are not limited to, the following: adding a protocol, adding, moving, or removing Customer Premises Equipment (CPE), changing addressing, filtering, and traffic prioritization schemes, optimizing

network routes, updating equipment software and/or configuration, including but not limited to firewall and VPN security devices, upgrading or downgrading bandwidth, implementing configuration changes for all agency-specific devices, maintaining a configuration database for all agency-specific devices, and auditing government router configurations.

Contractors shall provide IP Address Management as applicable. The Service Provider shall submit agency-completed American Registry for Internet Numbers (ARIN) justification requests for specified IP allocations to support the service offered.

Contractors shall monitor and control access to equipment under its control including limiting access to authorized personnel, implementing passwords, and user permissions as directed and approved by the agency.

Contractors shall perform off-site equipment configuration backups, to ensure the availability of recent configuration data for restoration purposes. Contractors shall provide the agency with secure access to backup logs as needed.

Contractors shall perform necessary hardware and software upgrades, updates, patch deployments and bug fixes as soon as they become available. Contractors shall implement, update, in coordination and agreement with the agency, and test new releases to resolve any security concerns, ensure compatibility with the agency environment, minimize service disruptions, and maintain equipment functionality.

Contractors shall provide preventative and corrective maintenance on agency-specific devices which include, but are not limited to, the following: monitor agency-specific network availability and quality of service (e.g., network delays, packet loss), monitor access circuit availability, and Quality of Service (QoS), monitor the government's edge router availability and performance, monitor transport service availability at the government's network equipment, monitor agency-specific network performance from government network equipment to government network equipment, monitor transport service availability up to the government's network equipment, monitor transport service performance from government network equipment to government network equipment, provide, monitor and manage circuits for out-of-band government network equipment management, open/close trouble ticket in agency's trouble ticketing system, open/close trouble ticket in Contractor's trouble ticketing system, troubleshoot access and transport services faults and coordinate faults resolution/repairs, troubleshoot government network equipment faults and coordinate resolution/repairs, troubleshoot agency-specific network faults, notify agency-specific network users of faults and maintenance via agency alerts, answer NOC Help Desk phones and provide Tier-1 support to agency-specific network users, provide Tier-1/Tier-2/Tier-3 support to agency NOC for Contractor access and transport services, and provide Tier-1/Tier-2/Tier-3 support to agency NOC for the components of the Agency's network that are managed by the Contractor.

Contractors shall provide the agency with real or near-time access to the following: installation schedule detailing the progress of activities such as the implementation of equipment, access and transport circuits, and ports, as applicable. Contractors shall allow the agency to track the provisioning process through completion at any time, network statistics and performance information including equipment data availability, throughput and delay statistics, CoS settings, and application-level performance information, trouble reporting and ticket tracking tools, and

security logs. Contractors shall provide inventory tracking tool(s) to maintain and track all agency circuit, transport service, and equipment inventory information.

Contractors shall provide the agency with secure access to current and historical information which includes, but is not limited to, the following: bandwidth and service quality information, burst analysis identifying under or over utilization instances, data errors, delay, reliability and data delivery summaries, end-to-end network views, exception analysis, link, port and device utilization, network statistics, protocol usage, CPU utilization, and traffic, port and protocol traffic, port, and protocol views.

Contractors shall maintain and repair Government Furnished Equipment (GFE) and Service-Related Equipment (SRE).

Contractors shall provide an agency-specific help desk services and shared or dedicated NOCs and SOC's to meet the agency requirements.

Contractors shall provide the agency with network testing which includes, but is not limited to, the following: MNS Contractor supports agency-specific development services to address agency's requirements to test equipment, software and applications on the Contractor's network prior to purchase and deployment, network testing will cover voice, data, and video technologies that include but are not limited to IP VPN and voice services, and testing will be performed at the agency's discretion and structured in collaboration with the Contractor.

C.7.3.1.6.2 Voice Managed Network Service (VMNS) / OPTIONAL

The Contractor shall support the transition of existing MNS services, as an option, for the agency's voice infrastructure to the GSA *EIS Contract* as Voice Managed Network Services (VMNS) solution, as described in Section C.2.8.1, Managed Network Service of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

In Phase 1, the agency will furnish, if it chooses to implement the VMNS option, the existing telephony network infrastructure as Government Furnished Property (GFP) to the Contractor. Section C.6.1.3 provides a description of the current EVS environment. Locations of the existing EVS telephony network infrastructure are identified in Table 6: IPVS within Section C.7.2.1.3.1 IPVS Locations, which includes the facility name, address, city, state, and zip code for each location.

Additional information for the existing EVS telephony network infrastructure is provided in Section J.3.1 VMNS Existing Infrastructure, as follows:

- Attachment J.3.1.1 Summary Telecom Inventory
- Attachment J.3.1.2 Telephony and Voice Mail License Distributions for the Avaya Communication Manager and Avaya Aura Messaging for the Denver (DEN) and Research Triangle Park (RTP) Data Centers
- Attachment J.3.1.3 Gateway Configurations
- Attachment J.3.1.4 Site Telephone Inventory

- Attachment J.3.1.5 RTP Asset Inventory
- Attachment J.3.1.6 DEN Asset Inventory
- Attachment J.3.1.7 RTP Network Diagram
- Attachment J.3.1.8 DEN Network Diagram

The Contractor's VMNS solution shall provide MNS for all the voice telephone GFE identified in Table 6: Summary Telecom Inventory in Section C.7.2.1.3.1 IPVS Locations, Section J.1 Pricing Workbook, and in the attached telephony network infrastructure documentation provided in Section J.3.1 VMNS Existing Infrastructure. The locations and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

The Contractor's VMNS solution shall operate and maintain the GFP based on performance levels, metrics, and SLAs for the transitioned services that shall be the same as those specified in the EIS Contract in Internet Protocol Voice Services (IPVS) Section C.2.2.1.4, Performance Metrics and in Section G.8.2.1, Service Performance SLAs.

C.7.3.1.6.3 SDWANS/ OPTIONAL

The Contractor shall support the SDWANS managed service, as an option, as described in Section C.2.8.10 of the EIS Contract, as well as any agency-specific requirements detailed in this SOW. The agency is looking at options for implementing SD-WAN, including connectivity, standards, technical capabilities, features, interfaces, and performance metrics that have been incorporated into the GSA EIS contract. This includes the opportunity to leverage broadband or cellular networks to reduce costs or achieve site networking redundancy. The scientific community at EPA is considering access to high speed scientific computing networks, such as NOAA's N-Wave or DOE's Energy Science Network (ESnet), using the SD-WAN solution.

The Contractor's SD-WAN solution shall include a Transformation Plan that includes the engineering, development, testing, accreditation, cost benefit analysis, implementation, maintenance, and managed network services support of the SD-WAN capability. The Transformation Plan shall be delivered after 90 days of the successful implementation of the VPNS for the agency and not to exceed 120 days after the successful implementation of the VPNS. The agency expects that traffic after 90 days of the successful implementation of the VPNS on the VPNS should allow the Contractor to evaluate the agency's traffic and usage.

The agency anticipates the migration to an SD-WAN operational model in a method that will keep operations unaltered and will lower the OPEX. The implementation of SD-WAN is not firmly scheduled, but it is mandatory that the Contractor be capable of providing the services described for the SD-WAN solution.

The Contractor's SD-WAN solution shall be compliant with federal security requirements including DHS TIC and associated use cases, as federally approved. Where TIC or other security requirements might prevent the implementation of an otherwise advantageous SD-WAN alternative, the Contractor's SD-WAN proposal shall identify security enhancements or

compensating controls designed to establish acceptable TIC use cases or assist the agency with a risk-based decision.

The Contractor's SD-WAN solution shall identify how the Contractor will deploy SD-WAN in the Contractor network access layer to enable rapid provisioning of bandwidth, dynamic path selection for specific application traffic, and policy control, and to reduce costs, enhance performance, or achieve site networking redundancy.

The Contractor's SD-WAN solution shall fully describe how their solutions align currently and/or strategically with the Metro Ethernet Forum (MEF) 3.0 or newer standards, as applicable. MEF 3.0 is a recognized emerging standard that meets many of EPA's strategic networking vision and functional objectives.

The Contractor's SD-WAN solution shall be capable of centralized control which shall provide the following functionality; Web Portals that shall support communication with the Contractor's BSS/OSS, network management systems, an enterprise portal that supports a view of the enterprise IP address range, support for service level SLA's, control of the individual EDGE SDP's, shall be capable of steering traffic based on performance required by each Functional Network or application, and shall be capable of defining policies for traffic steering and security protection supported by virtual firewalls (vFWs), and virtual identity providers (vIdP).

As the SD-WAN technical capabilities mature, the agency may introduce new requirements for features relating to SD-WAN.

C.7.3.1.7 Performance Metrics

C.7.3.1.7.1 Data Managed Network Service (DMNS)

The Contractor's DMNS solution shall meet the VPNS performance levels as specified in the *EIS Contract* in C.2.1.1.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs.

C.7.3.1.7.2 Voice Managed Network Service (VMNS) / OPTIONAL

The Contractor's VMNS solution shall meet the performance levels as specified in the *EIS Contract* in Internet Protocol Voice Services (IPVS), Section C.2.2.1.4 Performance Metrics and Section G.8.2.1 Service Performance SLAs.

C.7.3.1.7.3 SDWANS/ OPTIONAL

The Contractor's SDWANS solution shall meet the SDWANS performance levels as specified in the *EIS Contract* in C.2.8.10.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs.

C.7.3.2 Managed Trusted Internet Protocol Service (MTIPS)

The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet or exceed the requirements described in C.2.8.4: Managed Trusted Internet Protocol Service (MTIPS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractors shall deliver a like-for-like technology for the migration of these services to the GSA *EIS Contract*.

Locations identified in Section C.8.2.1: MTIPS Locations and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, or any other unforeseen reason.

C.7.3.2.1 MTIPS Locations

The Contractor's MTIPS solution shall have TIC portals for the agency at the following locations:

- William Jefferson Clinton (WJC) in Washington, DC
- National Computer Center (NCC) in Research Triangle Park, NC
- Denver Federal Center in Lakewood, CO (Optional)

C.7.3.2.2 Connectivity

The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet the requirements described in C.2.8.4.1.3: Connectivity within the Managed Trusted Internet Protocol Service (MTIPS) section in the *EIS Contract*.

C.7.3.2.3 Standards

The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet the requirements described in C.2.8.4.1.2: Standards within the Managed Trusted Internet Protocol Service (MTIPS) section in the *EIS Contract*.

C.7.3.2.4 Technical Capabilities

The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet the requirements described in C.2.8.4.1.4: Technical Capabilities within the Managed Trusted Internet Protocol Service (MTIPS) section in the *EIS Contract*.

The Contractor shall provide the following MTIPS capabilities as described in the *EIS Contract* in C.2.8.4.1.4.1: TIC Portal Capabilities and Section C.2.8.4.1.4.2: MTIPS Transport Collection and Distribution Capabilities.

The Contractor's MTIPS solution shall have a scalable 3 Gbps Port with 10 Gbps Ethernet Access Arrangement for each of the locations in Section C.8.2.1 MTIPS Locations.

The Contractor's MTIPS solution shall ensure that each TIC Portal provide full and complete geographic redundancy.

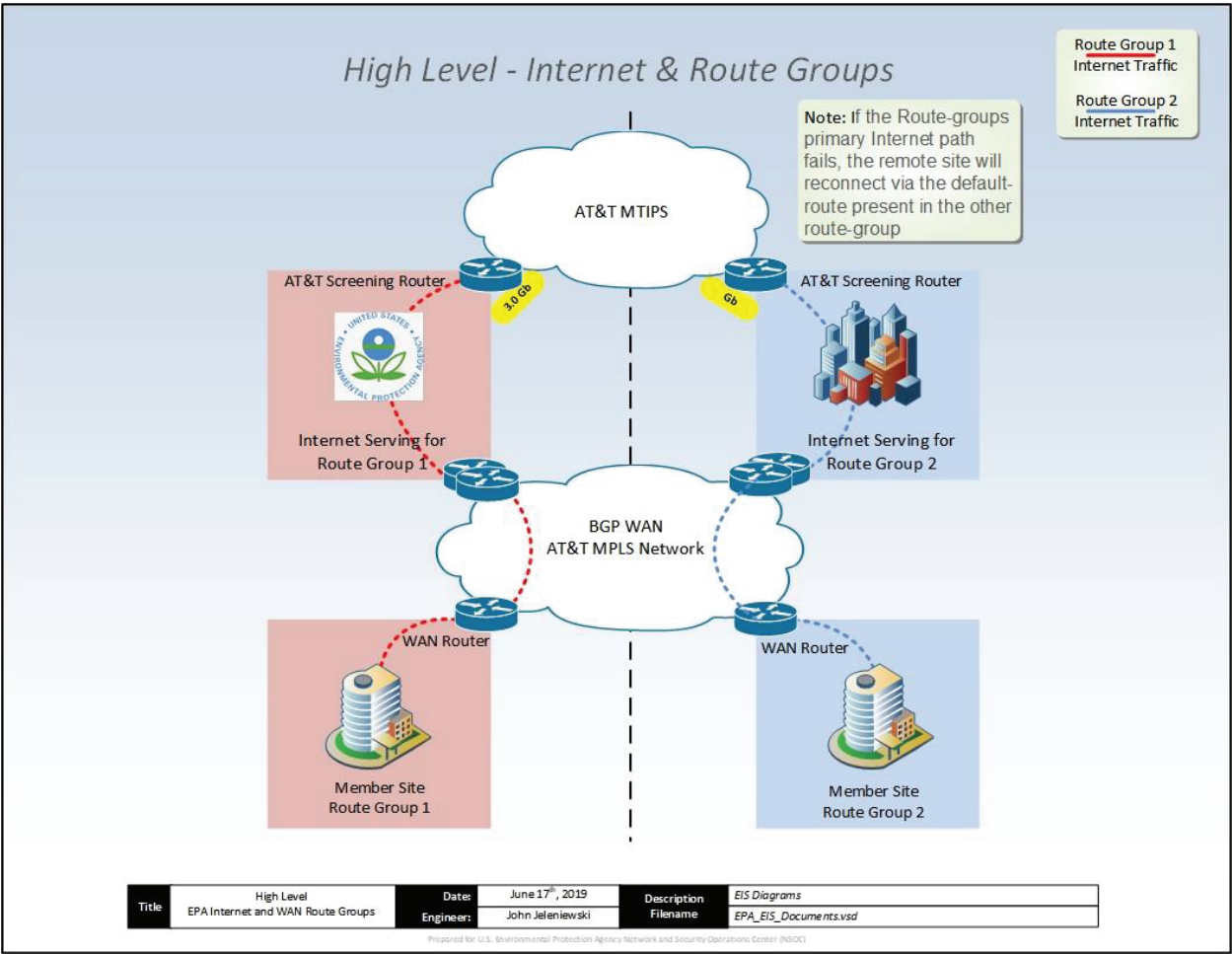
The Contractor's MTIPS solution shall serve as the primary Internet service for the following regions:

- William Jefferson Clinton (WJC) in Washington, DC
 - EPA defined Regions 1 – 5 as well as the Potomac Yard Data Center
- National Computer Center (NCC) in Research Triangle Park, NC
 - EPA define Regions 6 – 10, RTP Campus, and other Program Office locations

If EPA elects a third TIC Portal at Denver Federal Center, the Contractor shall deliver an optimal redistribution of the primary Internet services for EPA's Regions, Campuses, Data Centers and other Program Office locations.

The Contractor's Internet gateways shall always remain active and rely on a load-sharing feature entitled "route-groups" to forward Internet requests to the correct exit and thereby ensure routing symmetry as shown in Figure 1: High Level – Internet & Route Groups.

Figure 1: High Level - Internet & Route Groups



C.7.3.2.4.1 TIC Portal Capabilities

The Contractor shall provide the TIC Portal Capabilities that are specified mandatory as stated in Section C.2.8.4.1.4.1: TIC Portal Capabilities of the *EIS Contract*.

C.7.3.2.4.2 MTIPS Transport Collection and Distribution Capabilities

The Contractor's MTIPS solution shall transport Internet traffic securely to the Service Delivery Point (SDP). The Contractor's MPLS VPN network shall be the backbone transport service that connects the SDPs to the MTIPS solution. The Contractor's MPLS VPN service shall provide the agency with a secure, separate, and global connectivity to the TIC portal from the agency locations. The Contractor shall provide the following as stated in Section C.2.8.4.1.4.2: MTIPS Transport Collection and Distribution Capabilities of the *EIS Contract* for baseline requirements.

C.7.3.2.4.3 MTIPS Security Requirements

The Contractor shall ensure security requirements are met for the MTIPS as defined in the System Security Plan (see Section (see Section C.2.8.4.5.4), at a high impact level and shall support government security and authorization efforts. The Contractor shall provide the following as stated in Sections C.2.8.4.5: MTIPS Security Requirements and C.2.8.4.5.4: System Security Plan (SSP) of the *EIS Contract*.

C.7.3.2.5 Features

The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet the requirements described in C.2.8.4.2: Features within the Managed Trusted Internet Protocol Service (MTIPS) section in the *EIS Contract*.

C.7.3.2.6 Interfaces

The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet the requirements described in C.2.8.4.3: Interfaces within the Managed Trusted Internet Protocol Service (MTIPS) section in the *EIS Contract*.

C.7.3.2.7 Performance Metrics

The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet the performance levels as specified in the *EIS Contract* in C.2.8.4.4: Performance Metrics and Section G.8.2.1: Service Performance SLAs. The Contractor's Managed Trusted Internet Protocol Service (MTIPS) solution shall meet the performance levels and AQL of KPIs for MTIPS in Sections C.2.8.4.4.1 through C.2.8.4.4.2.

C.7.3.2.8 Special Requirements

C.7.3.2.8.1 MTIPS Remote Access / Optional

EPA is considering two different options for remote access under the GSA *EIS Contract*. The two options are: 1) a premised based Remote Access Service (see C.7.1.1.7.1) or 2) a Remote Access Service through the MTIPS described in this section. The Contractors shall provide solutions to both options. EPA will optionally elect to order one of these options.

The Contractor's MTIPS Remote Access shall provide a solution that meets or exceeds the requirements described in Section C.2.8.4.2, Features, 9. Remote Access, of the *EIS Contract* to include all applicable service descriptions, standards, technical capabilities, features, interfaces, and performance metrics defined in Section C.2.8.4: Managed Trusted Internet Protocol Service of the *EIS Contract*, as well as any other agency-specific requirements detailed in this SOW.

The Contractor's MTIPS Remote Access System shall:

- support 12,500 concurrent remote users, with the capability to expand to 20,000 concurrent remote users.
- be implemented at two separate EPA locations
 - the Potomac Yard Data Center located in Arlington, Virginia
 - the NCC located in Research Triangle Park, North Carolina
- maintain access to TIC portals
 - each TIC portal shall support 12,500 concurrent remote users with the capability to expand to 20,000 concurrent remote users

The Contractor's MTIPS Remote Access System shall include a test server for dedicated agency use for the purpose of:

- creating agency specific policies
- testing policies
- certifying configurations
- implementing agency profiles into the production environment
- mimicking the configurations to stage agencies in a pre-production environment

The Contractor's MTIPS Remote Access System shall include access to and use of the Contractor's:

- software modules,
- Remote Access Service NOC for management, support and monitoring capabilities
- Service Management Console

The Contractor's MTIPS Remote Access System shall include 24x7x365 telephone and email support, along with management, monitoring and availability reporting for the MTIPS Remote Access System.

C.7.3.3 Managed Security Services

C.7.3.3.1 Distributed Denial of Service (DDoS) Defense Service

The Contractor's DDoS Defense Service shall provide a solution that meets or exceeds the requirements described in Section C.2.8.5.2, Features, 1. Managed Prevention Service, h) Network Behavior Analysis of the EIS Contract, to include all applicable service descriptions, standards, technical capabilities, features, interfaces, and performance metrics defined in Section C.2.8.5: Managed Security Service of the EIS Contract, as well as any other agency-specific requirements detailed in this SOW.

The agency's definition of DDoS is a distributed denial of service attack directed toward the agency's IP addresses.

The Contractor's DDoS Defense Service shall provide a service that includes:

- DDoS attack detection
- DDoS attack mitigation Contractor
- Protection against volumetric attack traffic before reaching the agency sites

The Contractor's DDoS Defense Service shall provide:

- Traffic Anomaly Detection
- Misuse Anomalies
- Profiled Anomalies
- Cloud Signaling
- Mitigation through Network Packet Scrubbing facilities to include at a minimum:
 - Preauthorized Mitigation
 - Manual Mitigation

The Contractor's DDoS Defense Service shall consist of network detection device(s) which examines samples of agency traffic flow data from the Contractor's network for each address identified by the agency.

Upon detection, or agency notification to the Contractor of a perceived DDoS Attack, the Contractor's DDoS Defense Service shall reroute traffic targeted at an attacked host to a shared scrubbing device which then "scrubs" the rerouted traffic by dropping the suspected DDoS attack traffic.

C.7.3.3.2 Secured Email Gateway Service

The Contractor's Secured Email Gateway Service shall provide a solution that meets or exceeds the requirements described in Section C.2.8.5: Managed Security Service of the *EIS Contract*, to include all applicable service descriptions, standards, technical capabilities, features, interfaces, and performance metrics defined in, as well as any other agency-specific requirements detailed in this SOW. The Contractor shall include the EPA O365 Email Team on any Change Control discussion, meeting, or change control that will impact EPA Office 365 Email.

The Contractor's Secure Email Gateway Service solution shall provide gateway-based filtering that is designed to protect the agency against external threats such as spam, virus, malware and phishing attacks, and to help protect information that is leaving from the organization.

The Contractor's Secure Email Gateway Service solution shall provide at a minimum:

- Email firewall
- Quarantine
- Transport Layer Security (TLS)
- SPAM detection

- Virus protection
- Zero-hour anti-virus
- URL Defense that includes URL Rewrite
- Predictive Analysis
- Dynamic Malware Analysis Service
- Threat Insight Dashboard
- Target Attack Protection (TAP) for Attachment Defense that includes Dynamic Malware Analysis Service
- Threat Insight Dashboard
- Dynamic reputation
- Smart search
- Regulatory compliance
- Digital asset security
- Encryption

C.7.3.3.3 Security Operations Center (SOC) Managed Security Services

The Contractor's Managed Security Operations Center (SOC) shall provide a solution that meets or exceeds the requirements described in Section C.2.8.5: Managed Security Service of the *EIS Contract*, to include all applicable service descriptions, standards, technical capabilities, features, interfaces, and performance metrics defined in, as well as any other agency-specific requirements detailed in this SOW.

The Contractor shall describe the design of the Managed SOC that meets the needs of the agency by providing analysis/correlation and management structure to mitigate the threat presented by attacks based on industry standards, best practices, etc.

The Contractor's shall detail but not be limited to explaining the methodologies for the staffing, incident handling, proactive monitoring, and alerting of the SOC.

The Contractor's Managed SOC shall include and manage a set of tools, appliances and processes that collect, reduce, normalize, correlate, fuse, and manage event data.

The Contractor's SOC tools shall also provide reports that are based on past experiences and best practices, but as a minimum, support authorities / analysts by identifying security events of interest that may be negatively affecting the agency environment.

The Contractor Managed SOC security authorities / analysts shall react to and trigger appropriate control mechanisms, thus creating the Rapid Response Loop.

The Contractor shall provide trained, qualified, and cleared staff (U.S. citizens) to support security functions 24x7.

C.7.3.3.4 Performance Metrics

C.7.3.3.4.1 DDoS MSS

The MSS performance levels and AQL of KPI in Section C.2.8.5.4.1 Managed Security Service Performance Metrics of the *EIS Contract* are mandatory unless marked optional.

In addition, the Contractor shall meet the requirements listed in Section J.3.2 DDoS Service Level Requirements.

C.7.3.3.4.2 Secured Email Gateway MSS

The MSS performance levels and AQL of KPI in Section C.2.8.5.4.1 Managed Security Service Performance Metrics of the *EIS Contract* are mandatory unless marked optional. Service credit tables are provided in Section G.8 Service Level Management of this SOW.

In addition, the Contractor shall meet the following Service Level Requirements (SLR):

C.7.3.3.4.2.1 Filtering System Availability Service Level Requirements

Contractor shall warrant at least 99.999% System Availability for the filtering and delivery of email during each calendar month, excluding Scheduled Maintenance Window and Emergency Maintenance. This is defined as the percentage of time in a calendar month that the network is able to receive and process email messages, including emergency and planned maintenance.

If the email System Availability is less than 99.999%, and if EPA is in material compliance with its obligations under the Agreement and this SLA, Contractor shall provide EPA with a Service Credit for the month in which the failure to meet the email System Availability SLA has occurred, as provided in Section G.8.1 SLA Credits and Adjustments.

C.7.3.3.4.2.2 Email Delivery Service Level Requirements

The Contractor shall warrant that the average of Email Delivery (as defined below) times, as measured in minutes over a calendar month, will be one (1) minute or less.

For purposes of this SLR “Email Delivery” is defined as the elapsed time from when a business email enters the Security Services network to when it exits the Security Services network. Email delivery latency is the average of total email delivery time measured in minutes over a calendar month. Email delivery time is measured and recorded every 5 minutes, then sorted by elapsed time. The fastest 95% of measurements are used to create the average for the calendar month. Email delivery latency applies only to legitimate business email (non-bulk email) delivered to valid email accounts.

This SLR shall not apply to:

- Delivery of email to quarantine or archive
- Email in deferral queues

- Denial of Service attacks (DoS)
- Email loops

This SLR shall only apply to legitimate business email (i.e. not to any spam email as defined under applicable law for commercial messages including the CAN-SPAM Act) delivered to valid Mailbox accounts that are contracted for the Security Services.

EPA will not have any remedies under this SLA to the extent any SLA claim hereunder is due to (i) delivery of email to quarantine; (ii) email in deferral queues; or (iii) email loops.

If in any calendar month the Email Delivery SLR is not met and if EPA is in material compliance with its obligations, the Contractor shall provide EPA with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit shall be calculated in accordance with the table in Section G.8.1 SLA Credits and Adjustments.

C.7.3.3.4.2.3 Virus Filtering Service Level Requirements

The Contractor shall warrant that the Security Services will Filter (as defined below) 100% of all **known Viruses** (as defined below) contained in an inbound email to an EPA Mailbox for which a Security Services subscription has been purchased. The Contractor shall warrant that the Security Services will Filter 100% of all Viruses contained in an outbound email from an EPA Mailbox for which a Security Services subscription has been purchased.

For purposes of this SLR, the following definitions shall apply:

This SLR shall not apply to (i) text messages that use fraudulent claims to deceive the EPA and/or prompt the EPA to action (such as phishing); (ii) a binary or executable code installed or run by an end user that gathers information for sales and marketing purposes (such as spyware); (iii) a virus that has been detected and has been cleaned by other virus scanning products; (iv) an ineffective or inactive virus contained in a bounced email; (v) a Virus-infected email that is quarantined by the Service but is subsequently delivered to an end user or administrator by such end user or administrator; (vi) emails containing attachments that are password protected, encrypted or otherwise under an end user's control; or (vii) any action by a Contractor end user or administrator that results in deliberate self-infection.

If a validated Infection occurs in any calendar month, and if EPA is in material compliance with its obligations under the SOW, the Contractor shall provide Customer with a Service Credit for the month in which the failure to meet this SLA has occurred. The Service Credit shall be calculated in accordance with the table in Section G.8.1 SLA Credits and Adjustments.

C.7.3.3.4.2.4 Spam Inbound Effectiveness Service Level Requirements

The Contractor shall warrant that the Security Services will detect 99% of inbound spam in each calendar month. This SLA does not apply to false negatives to invalid Mailboxes. The Contractor shall make a good faith estimation of the spam capture rate based on the regular and prompt submission to the Security Services support center of all false negatives to report spam missed by Security Services.

The Contractor shall estimate the percentage of spam detected by the Security Services by dividing the number of spam emails identified by the Security Services as recorded in the Security Services report logs by all spam emails sent to EPA. The Contractor shall estimate all spam emails sent to EPA by adding the number of spam messages (false negatives) missed by the Security Services and reported to the Security Services support team to the number of spam emails detected by the Security Services.

If the Contractor and/or EPA detects less than 99% of inbound spam in any calendar month, and if EPA is in material compliance with its obligations under the SOW, the Contractor shall provide EPA with a Service Credit for the month in which the failure to meet this SLR has occurred. The Service Credit will be calculated in accordance with the table in Section G.8.1 SLA Credits and Adjustments.

C.7.3.3.4.2.5 Spam Outbound Effectiveness Service Level Requirements

The Contractor shall warrant that the Security Services will detect 95% of outbound spam in each calendar month. The Contractor shall make a good faith estimation of the spam capture rate based on the regular and prompt submission to the Security Services support center of all false negatives to report spam missed by Security Services.

The Contractor shall estimate the percentage of spam detected by the Security Services by dividing the number of outbound spam emails identified by the Security Services as recorded in the Security Services report logs by all outbound emails sent from the EPA through the Security Services. The Contractor shall calculate the total number of emails sent from EPA through the Security Services in each calendar month.

If the Contractor and/or EPA detects less than 95% of outbound spam in any calendar month, and if EPA is in material compliance with its obligations under the SOW, the Contractor shall provide EPA with a Service Credit for the month in which the failure to meet this SLR has occurred. The Service Credit will be calculated in accordance with the table in Section G.8.1 SLA Credits and Adjustments.

C.7.3.3.4.2.6 False Positive Service Level Requirements

The Contractor shall warrant that the ratio of legitimate business email incorrectly identified as spam by the Security Services to all email processed by the Security Services for the EPA in any calendar month will not be greater than 1:350,000. The Contractor shall make a good faith estimation of the false positive ratio based on evidence timely supplied by EPA.

This SLR shall not apply to (i) spam email (as defined as under applicable law for commercial messages including the CAN-SPAM Act under U.S. federal law), personal email from an individual end user of EPA outside of the scope of such individual end user's employment or independent contractor services for the benefit of EPA, pornographic email; or (ii) emails blocked by a policy rule, reputation filtering, or SMTP connection filtering.

If the Contractor does not meet this SLA in any calendar month and if EPA is in material compliance with its obligations under the SOW, the Contractor shall provide EPA with a Service

Credit for the month in which the failure to meet this SLA has occurred. The Service Credit shall be calculated in accordance with the table in Section G.8.1 SLA Credits and Adjustments.

C.7.3.3.4.2.7 Service Level Requirements Definitions

“Filter” means to detect and block or quarantine all email messages with Viruses that (i) match an available virus signature; (ii) are identifiable by industry standard anti-virus engine heuristics; or (iii) are propagated through registered attachment types.

“Infection” means if an inbound email to an EPA Mailbox is delivered with a Virus, or if an outbound email from an EPA Mailbox is processed through the Security Services with a Virus without being quarantined.

“Scheduled Maintenance Window” means the window during which weekly scheduled maintenance of the Products may be performed. The Scheduled Maintenance Window is between the hours of Friday 9:00 p.m. to Saturday 5:00 a.m. Pacific time.

“Emergency Maintenance” means any time outside of Scheduled Maintenance Window that Supplier is required to apply urgent patches or fixes or undertake other urgent maintenance activities.

“System Availability” means the percentage of total time during which a Service is available to EPA, excluding Scheduled Maintenance Window and Emergency Maintenance.

“Service Credit” means the percentage of the monthly Subscription Fees paid or payable for the Products that is awarded to EPA for a validated claim associated with that portion of the Products related to breach of the applicable SLA during that month.

“Virus” means a binary or executable code whose purpose is to gather information from the infected host (such as trojans), change or destroy data on the infected host, use inordinate system resources in the form of memory, disk space, network bandwidth or CPU cycles on the infected host, use the infected host to replicate itself to other hosts, or provide control or access to any of the infected host’s system resources.

C.7.3.3.4.3 SOC MSS

The MSS performance levels and AQL of KPI in Section C.2.8.5.4.1 Managed Security Service Performance Metrics of the *EIS Contract* are mandatory unless marked optional.

C.7.4 Access Arrangements Tasks

The Contractor’s Access Arrangements (AA) solution shall meet the requirements described in C.2.9: Access Arrangements (AA) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The agency has given preference for cost effective implementations of Ethernet Access Arrangements to the WAN. The agency also desires to implement wireless technologies to reduce last mile charges for buildouts to support the agency infrastructure and to reduce monthly reoccurring charges for supporting backup communication devices on a pay as needed basis.

The Contractor shall provide a cost-effective comparative AA for the migration of these AA to the GSA *EIS Contract*. Depending on availability and price, EPA plans to upgrade its TDM AA services to VPNS, both NxT1s as well as DS-3s, to Ethernet.

The Access Arrangements (AA) that is presently in place and that is considered to be transitioned is identified in Section J.1: Pricing Workbook (see the tab on bandwidth growth which includes how the TDM circuits map into different Ethernet bandwidths). Locations identified in Section J.1 and requirements are subject to change due to agency staffing level changes, agency location closures, additions of new locations, cost considerations, or any other unforeseen reason. Where no access arrangement is specified, the Contractors shall propose appropriate access technologies.

C.7.4.1 Connectivity

The Contractor's Access Arrangements (AA) solution shall meet the connectivity requirements as described in C.2.9.1.3: Connectivity within Access Arrangements (AA) of the *EIS Contract*.

C.7.4.2 Standards

The Contractor's Access Arrangements (AA) solution shall meet the requirements described in C.2.9.1.2: Standards within the Access Arrangements (AA) section in the *EIS Contract*.

C.7.4.3 Technical Capabilities

The Contractor's Access Arrangements (AA) solution shall meet the requirements described in C.2.9.1.4: Technical Capabilities within the Access Arrangements (AA) section in the *EIS Contract*.

C.7.4.4 Access Diversity and Avoidance

The Contractor's proposed Access Diversity and Avoidance solution shall meet the requirements described in C.2.9.2: Access Diversity and Avoidance section in the *EIS Contract*.

C.7.4.4.1 Research Triangle Park Access Diversity and Avoidance

The Contractor's Access Diversity and Avoidance solution shall provide for the National Computer Center (NCC) located at Research Triangle Park (RTP), dual 2 Gbps Port Ethernet connections to the WAN, through diverse 10Gb Access fiber paths onto the Research Triangle Park (RTP) campus. These circuits shall provide redundancy for one another as well as local diversity for the RTP Campus. These circuits shall connect to separate facilities on the RTP

Campus (NCC and Campus C-building) and shall be served by a separate local telco point of presence (POP).

C.7.4.5 Interfaces

The Contractor's Interfaces for Access Diversity solution shall meet the requirements described in C.2.9.3: Access Diversity and Avoidance section in the *EIS Contract*.

C.7.4.6 Special Requirements

C.7.4.6.1 Broadband and Cellular Access Arrangement

The Contractor's Access Arrangements (AA) solution shall include broadband (high-speed cable and FTTP) cellular access arrangements that interconnect fixed endpoints such as cable modems, Mi-Fi wireless routers, wireless broadband devices, and other SRE equipment. The Contractor's Access Arrangements (AA) solution shall provide the best available cellular technology, either 4G, 4G/LTE or 5G technology, wherever that technology is available within CONUS and OCONUS. The Contractor's high-speed cable and FTTP AA shall provide the highest upstream and highest downstream bandwidth based on the location. The Contractor's Access Arrangements (AA) solution shall not restrict number of users on the cellular AA.

The section J.1 Pricing Workbook includes a separate tab for pricing of all requested broadband AAs embedded with IPS and VPNS ports. These are VPNS and IPS TUCs and not AA TUCs. See the workbook instructions for further details.

C.7.5 Cable and Wiring Service (CWS) Tasks

The Contractor's Cable and Wiring Service (CWS) solution shall meet the requirements described in C.2.12: Cable and Wiring Service (CWS) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The agency will utilize the Cable and Wiring Service (CWS) to support a wide range of cable and wiring requirements to enable the agency to meet mission critical responsibilities. Specific requirements for each location will be specified in the Task Order Specific Requirements associated with the work to be completed at the location. The Contractor shall include an approach to site surveys that may or may not be needed by the customer(s) at various locations.

The Contractor's Cable and Wiring Service (CWS) shall include as-built documentation, if requested on the Task Order, to be delivered within 60 days of the completion of work, for any work performed on the agency locations in Section J.1 Pricing Workbook. The Contractor shall submit a detailed cost estimate, project plan, test plan, and project timelines to the agency for review and approval.

C.7.5.1 Special Requirements

The Contractor shall provide Cabling and Wiring for the Task Order Specific Requirements to support the requirements of the agency for each of the following scenarios listed.

Description	Charging Unit	Notes
PDU Strip Rairtan PX2-1497V or equivalent	Each	Includes labor to install the strip
6 Outlet APC Horizontal Power Strip or equivalent	Each	Includes labor to install the strip
Equipment Rack, Standard two-post 19-inch-wide x 84 inches tall	Each	Includes labor to mount the rack in standard concrete floors
Wall-mount cabinets, 24 inches wide x 24 inches deep x 48 inches high	Each	Includes labor to mount the rack on standard drywall wall
Patch Panels and Cable Management, metal or high impact plastic, with manufacturer's standard finish in black	Each	Includes labor
Patch Cords, factory made certified Category 6A plenum rated patch cords with snag resistant stress relief boots, 5 foot	Each	Includes labor
Patch Cords, factory made certified Category 6A plenum rated patch cords with snag resistant stress relief boots, 8 foot	Each	Includes labor
Patch Cords, factory made certified Category 6A plenum rated patch cords with snag resistant stress relief boots, 10 foot	Each	Includes labor
Patch Cords, factory made certified Category 6A plenum rated patch cords with snag resistant stress relief boots, 12 foot	Each	Includes labor
Patch Cords, factory made certified Category 6A plenum rated patch cords with snag resistant stress relief boots, 14 foot	Each	Includes labor
Patch Cords, factory made certified Category 6A plenum rated patch cords with snag resistant stress relief boots, 16 foot	Each	Includes labor
Faceplates, accommodate 4 pair copper, optical fiber, and coaxial snap-in connecting hardware, with clear window	Each	Includes labor

displays covering outlet labels, and available in multiple gang and port variations		
Category 6 Jack Insert, to accommodate Category 6A, 4 pair, 100-ohm, 500 megahertz (MHz) balanced Unshielded Twisted Pair (UTP). Terminations are EIA/TIA 568A	Each	Includes labor
Blank Jack Insert	Each	Includes labor
Horizontal Cabling, consisting of cabling and connecting hardware between the floor or space serving Remote Wiring Closet (RWC) and Work Area Outlets (WAO's). Each Work Station Outlet (WAO) will receive a Category 6A, 4 pair, non-plenum, 100-ohm, 500 megahertz (MHz) balanced Unshielded Twisted Pair (UTP), blue in color, terminated in Patch Panels on connecting EIA/TIA 568A hardware of same performance category or higher and per manufacturer instructions, up to 100 meters in length	Each	Includes labor
Horizontal Cabling, consisting of cabling and connecting hardware between the floor or space serving Remote Wiring Closet (RWC) and Work Area Outlets (WAO's). Each Work Station Outlet (WAO) will receive a Category 6A, 4 pair, plenum rated, 100-ohm, 500 megahertz (MHz) balanced Unshielded Twisted Pair (UTP), blue in color, terminated in Patch Panels on connecting EIA/TIA 568A hardware of same performance category or higher and per manufacturer instructions, up to 100 meters in length	Each	Includes labor
Riser or Feeder Cabling will consist of Category 3, 25 pair 100 ohm, balanced Shielded and Unshielded Twisted Pair (UTP), plenum rated cable terminated on rack mount 100 IDC blocks.	Per Foot	Includes labor and terminations
Riser or Feeder Cabling will consist of Category 3, 50 pair 100 ohm, balanced Shielded and Unshielded Twisted Pair (UTP), plenum rated cable terminated on rack mount 100 IDC blocks.	Per Foot	Includes labor and terminations
Riser or Feeder Cabling will consist of Category 3, 100 pair, 100 ohm, balanced Shielded and Unshielded Twisted Pair	Per Foot	Includes labor and terminations

(UTP), plenum rated cable terminated on rack mount 100 IDC blocks.		
Demarcation Extension, Conduit Installation, to include but not be limited to; 1ft - 50ft 2in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 1ft - 50ft 3in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 51ft – 100ft 2in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 51ft – 100ft 3in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 101ft-150ft 2in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 101ft-150ft 3in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 151ft-200ft 2in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 151ft-200ft 3in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 201ft-250ft 2in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 201ft-250ft 3in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 251ft-300ft 2in EMT	Each	Includes labor
Demarcation Extension, Conduit Installation, to include but not be limited to; 251ft-300ft 3in EMT	Each	Includes labor

EPA will:

- Provide appropriate access to the work areas and facilities from the hours of 8:00 am to 4:30 pm Monday through Friday, local time.
- Provide access for deliveries to the facilities from the hours of 9:00 am to 3:00 pm, Monday through Friday, local time. If necessary, EPA site staff will coordinate with other Federal Agencies or Building Owners as necessary to facilitate deliveries.

- Ensure facility requirements are met prior to the work start date per the Contractor provided implementation schedule.
- Provide Telecommunication Ground Bus-bar (TGB) attached to building ground in each LAN closet and the computer room.
- Make available sufficient dry and secure storage space at each facility to allow ready access to project materials prior to installation start.
- Provide access to elevators and coordinate their use with the other tenants or building owners for equipment movement.
- Provide trash dumpsters to remove debris from the site, as well as have the dumpsters removed and replaced to prevent trash overflow.

Access to all telecom closets, computer rooms and other works areas will be provided for the duration of any installation phase and cutovers which will include nights and weekends, as required.

The Contractor, upon completion of each task, shall remove all extraneous material and clean up the work area. The Contractor shall keep the work area clean and maintain a safe working environment.

C.7.5.2 Performance Metrics

The Contractor's Cable and Wiring Service (CWS) shall meet the performance levels and acceptable quality level (AQL) of Key Performance Indicators (KPIs) for the Cable and Wiring Service (CWS), as stated in the table below. The agency may state specific AQL/KPI/SLAs on the specific Task Order basis, based on the specific requirements of the project.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	How Measured
Response to Request	Routine	10 Business Days	≥ 10 days	See Note 1
Response to Request	Critical	5 Business Days	≥ 5 days	See Note 1
Site Survey	Routine	10 Business Days within Response to Request	≥ 10 days	See Note 1
Site Survey	Critical	5 Business Days within Response to Request	≥ 5 Business Days	See Note 1
Detailed Cost Estimate, Project Plan, Test Plan,	Routine	10 Business Days within Site Survey	≥ 10 Business Days	See Note 1

and Project Timelines				
Detailed Cost Estimate, Project Plan, Test Plan, and Project Timelines	Critical	5 Business Days within Response to Request	≥ 5 days	See Note 1
As Built Documentation	Routine	60 Calendar Days after completion of the project	≥ 60 days	See Note 1

Note 1 ; Notification begins when the Ordering Official notifies the Contractor by email, voice mail, telephone conversation, or conversation and follows up in email within two days in the case of voice mail, telephone conversation, or conversation.

C.7.6 Service-Related Equipment (SRE) Tasks

The Contractor's Service-Related Equipment (SRE) solution shall meet the requirements described in C.2.10 Service-Related Equipment (SRE) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW. The Contractor's Service-Related Equipment (SRE) solution shall be capable of supporting SD-WAN. The agency is seeking the purchase, installation, de-installation, and maintenance and support of Service-Related Equipment (SRE).

The Contractor shall install SRE as required to meet the specifications of the terminal equipment located at the government SDP. The details and specifications for the interfaces at each SDP will be provided in each service order. The Contractor's Service-Related Equipment (SRE) solution shall meet and comply with the requirements for Payment Methods as described in Section B.2.10.4 Payment Methods of the *EIS Contract*. The SRE required to deliver the services under this SOW will be purchased in accordance with the *EIS Contract* Section B.2.10.3.1 SRE Pricing Elements Reference Table, unless otherwise stated in the agency-specific requirements. The SRE to be provided by the Contractor shall be new and not refurbished.

The Contractor shall develop and maintain an online catalog of SRE offerings and pricing in accordance with the requirements specified in Section B.1.3 and B.2.10.1 of the *EIS Contract*.

The Contractor shall provide product classes and discounts off the Official List Price (OPL) for all SRE and in addition to provide prices for all required VoIP phones listed in Section 7.2.1.3.3 Table 8 - IP Telephone Breakdown and as per the instructions in the Section J.1 Pricing Workbook.

C.7.7 Service-Related Labor Tasks

It is understood that the EIS services as defined in Sections C.2.1 through C.2.10, and in Section C.2.12 of the *EIS Contract* include all service-related labor necessary to implement the services. Service-related labor under the *EIS Contract* shall be incidental to the EIS services being implemented or supported. Labor for construction, alteration, and repair (if applicable) is only in scope as necessary to offer a complete a telecommunications solution if it is integral to and necessary for the effort stated in the task order. The allowed scope for labor service is described in Section C.2.11 of the *EIS Contract*. Job descriptions for EIS labor categories are presented in Section J.5 of the *EIS Contract*. Labor services performed under the *EIS Contract* shall be either time and materials (T&M) or fixed price.

C.7.8 System Security Requirements/Tasks

The Contractor's System Security Requirements solution shall meet the requirements described in C.1.8.7: System Security Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractor will also comply with the Additional Security Requirements stated in C.1.8.7.6 of the *EIS Contract*.

C.7.8.1 System Security Compliance Requirements

The Contractor's System Security Compliance Requirements solution shall meet the requirements described in C.1.8.7.1: System Security Compliance Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.8.2 Security Compliance Requirements

The Contractor's System Security Compliance Requirements solution shall meet the requirements described in C.1.8.7.1: System Security Compliance Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.8.3 Security Assessment and Authorization (Security A&A)

The Contractor's Security Assessment and Authorization (Security A&A) shall meet the requirements described in C.1.8.7.3: Security Assessment and Authorization (Security A&A) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.8.4 System Security Plan (SSP)

The Contractor's System Security Plan (SSP) shall meet the requirements described in C.1.8.7.4: System Security Plan (SSP) of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.8.5 System Security Plan Deliverables

The Contractor's System Security Plan Deliverables shall meet the requirements described in C.1.8.7.5: System Security Plan Deliverables of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.8.6 Additional Security Requirements

The Contractor's Additional Security Requirements shall meet the requirements described in C.1.8.7.6: Additional Security Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.8.7 Personnel Background Investigation Requirements

The Contractor's Personnel Background Investigation Requirements shall meet the requirements described in C.1.8.7.7: Personnel Background Investigation Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

It is understood that the agency will be responsible for the cost of any required background investigations.

C.7.8.8 Protection of Government Property

The *EIS Contractor* shall be responsible for properly protecting all information used, gathered, or developed because of this contract. The *EIS Contractor* shall implement procedures that ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of sensitive government information, data, and/or equipment. The *EIS Contractor* procedures shall be consistent with Government and GSA policies, including agency specified directive, Information Technology Security Policy, OMB Circular A-130 (Management of Federal Information Resources), OMB M-06-16, OMB M-07-16, HSPD12, and the Privacy Act. In addition, during all activities and operations on Government premises the Contractor shall comply with the procedures, policies, rules, and regulations governing the conduct of personnel or protection of Government facilities and data as expressed by GSA, written or oral.

All Contractor's personnel shall take the annual EPA IT Security Awareness Training Course before being allowed access to EPA computers and networks.

The *EIS Contractor* shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally controlled EPA facility or access to a federal EPA information system.

C.7.8.9 Personnel Security Clearances

Personnel assigned under this task order must have the required clearance for the position. Clearance level and additional guidance is provided on the Department of Defense Contract Security Classification Specification (DD Form 254).

C.7.9 National Policy Requirements Tasks

The Contractor's National Policy Requirements shall meet the requirements described in C.1.8.8 National Policy Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.7.9.1 National Security and Emergency Preparedness

The Contractor's National Security and Emergency Preparedness (NS/EP) solution shall meet the requirements described in EIS Section C.1.8.8, National Policy Requirements, and in EIS Section G.11, National Security and Emergency Preparedness, as well as any agency-specific requirements detailed in this SOW.

The Contractor shall provide high availability options for load-balancing, fail-over protection and diverse access points to service provider's Point(s) of Presence under NS/EP.

C.7.10 Technical Support Tasks

The Contractor's Technical Support shall meet the requirements described in C.1.8.9: Technical Support Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The *EIS Contractor* shall provide customer technical support as a component of each of its EIS services. For detailed requirements, please see Section G.6.2: Customer Service Office and Technical Support, and Section G.6.4: Trouble Ticket Management of the *EIS Contract*.

C.8 Transition Tasks

The Contractor's Transition shall meet the requirements described in C.3: Transition of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.8.1 Transition Roles and Responsibilities

C.8.1.1 Government's Role in Transition

The Government's Role in Transition shall meet the requirements described in C.3.1.1: Government's Role in Transition of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.8.1.2 Contractor's Role in Transition

The Contractor's Role in the Transition shall meet the requirements described in C.3.1.2: Contractor's Role in the Transition of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.8.2 Transition On Tasks

The Contractor's Role in the Transition On shall meet the requirements described in C.3.2, C.3.2.1, C.3.2.2, C.3.2.3, and C.3.2.4: Transition On of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractor shall provide a detailed Transition Plan for transitioning services to the GSA *EIS Contract*. To ensure that the TO is in place in a thorough and orderly manner, the Contractor shall provide a draft transition plan with its proposal and a final plan within 60 calendar days of TO award. The final Transition Plan shall incorporate feedback from EPA.

The Transition Plan shall address, at minimum, how the Contractor will achieve the following topics and objectives of the plan:

Executive Summary

The Contractor shall provide an executive summary for the transition-on plan, that will describe the transition plan at a high level and what the plan should accomplish. This section of the transition plan should include an overview and history of the contract, who the contract is transitioning to, and the timeframe/period of transition.

C.8.2.1 Transition Approach

The Contractor shall provide a transition-on plan that discusses the overall approach to the transition. Some items which must be discussed are: will you scale up your staff during the transition or will you bring in additional staff to handle and manage the transition? How long is the transition? What are your assumptions (i.e., the staff of the old contractor will be available onsite to participate in the transition and participate in the knowledge transfer, etc.)? The Contractor shall provide a list of all requirements from EPA and a matrix listing the major responsibilities of the EPA and the Contractor to execute the transition successfully.

C.8.2.1.1 Transition Gateway

The Contractor shall describe how they intend to connect the legacy network to the agency's network for the initial implementation and through the agency's EIS transition period. The Contractor shall provide gateways between the legacy network and agency network to provide access continuity from all sites to enterprise services such as the Internet, cloud, data centers, and Legacy sites to SDPs during transition. SDPs shall interconnect to both the legacy network and agency network during transition and transformations. The Contractor shall detail within the Contractor's transition plan; for example, how SDPs will be placed at regional hubs or interconnections will be made between the legacy network and the agency network. The Contractor shall initially provide 10 Gbps Access Arrangements for each gateway. The

Contractor shall allow transport to be rapidly provisioned throughout the transition period for the Transition Gateways.

C.8.2.1.1.1 Transition Gateway Performance Metrics

The Contractor shall ensure that the maximum latency between SDPs and the legacy network shall be based on the following specific KPIs. The Contractor shall participate in all discussions with the agency and the legacy network service provider to mitigate latency issues identified by agency or the Contractor.

Transition Gateway Service Level Requirements

KPI	Service Level	Severity Level	Performance Threshold	AQL	Notes
Av (Legacy Gateway)	n/a	n/a	99.9%	≥ 99.9%	See Note 2
Latency (CONUS)	Routine	n/a	70 ms	≤ 70 ms	See Note 1
Latency (OCONUS)	Routine	n/a	150 ms	≤ 150 ms	See Note 1
Time to Restore	Without Dispatch	n/a	4 hours	≤ 4 hours	See Note 3
	With Dispatch	n/a	8 hours	≤ 8 hours	

1. Latency value is the average round trip transmission between Legacy Gateway to its CONUS sites. The latency metric does not apply for DSL, Cable High Speed, Wireless, and Satellite access methods. The relevant standards are RFC 1242 and RFC 2285. The Contractor may propose to the agency a more cost-effective test and measurement technique alternatives that meet or exceed the requirements in RFC 1242 and RFC 2285.
2. Transition Gateway availability is measured end-to-end and calculated as a percentage of the total reporting interval time that the Transition Gateway is operationally available to the agency. Availability is computed by the following formula:

$$Availability = \frac{[RI(LUTN) - COT(LUTN)]}{RI(LUTN)} \times 100$$

3. See Section G.8.2 for the definitions and measurement guidelines.

C.8.2.2 Transition Team Organization

The Contractor shall provide in the transition-on plan an organizational chart showing all resources and their roles in the transition (i.e., Transition Project Manager, Program Manager, Network Engineer, etc.). The Contractor shall demonstrate that sufficient workforce of qualified staff with the necessary skill sets and geographic reach is available and committed to the transition.

C.8.2.3 Governance and Reporting

The Contractor shall include plans to facilitate the necessary monitoring and reporting via monthly and ad hoc reporting capabilities as well as monitoring of orders, implementation, and inventory related to the transition. The Contractor shall discuss how the Contractor will incorporate the EPA Change Management Structure processes to ensure appropriate structure and collaboration between the Contractor and EPA. The Contractor shall identify the methods to be used to conduct the asset inventory validation.

C.8.2.4 Quality Control

The Contractor shall address the Contractor's Quality Control Plan including the system, processes, techniques, customer feedback collection, monitoring, tools and techniques, reporting, customer feedback collection, and corrective action processes.

C.8.2.5 Communications

The Contractor shall include a comprehensive methodology to promote enriched communications and education between the Contractor, EPA stakeholders, and incumbent Contractors. The Contractor's Transition Plan shall ensure escalation procedures with EPA and the incumbent Contractors to support proper implementation, issue resolution and reduce ambiguity.

C.8.2.6 Workforce Transition

The Contractor shall provide in the transition-on plan details about the workforce that is being transitioned, if any.

C.8.2.7 Work Execution During Transition

The Contractor shall discuss the level of work which is to be performed during the transition period and the impact of the transition on that work. The Contractor shall discuss how the Contractor operational processes will be tested for verification of full operational capability.

C.8.2.8 Subcontracts

The Contractor shall document all the existing contracts and if/how they will be transitioned on. It shall contain this information in a table format (subcontract agreements, software/hardware maintenance contracts, etc.).

C.8.2.9 Property Transition

C.8.2.9.1 Government Furnished Equipment (GFE)

The Contractor shall describe the transition of any equipment for a scenario where the agency provides the contractor with government property. This property may include hardware such as laptops/PCs and security badges. The Contractor shall address details of how the Contractor intends to support the existing telephony network infrastructure.

C.8.2.9.2 Incumbent Owned Equipment

The Contractor shall describe the transition of any equipment owned by the incumbent contractor.

C.8.2.9.3 Intellectual Property

The Contractor shall describe how intellectual property will be handled as part of the transfer process. Intellectual property may include various documentation, supplier and subcontractor information, service agreements, or original designs or plans.

C.8.2.10 User Accounts and Passwords

The Contractor shall describe how any accounts will be transitioned, who they will be transitioned to (i.e., system administrator accounts). The Contractor shall provide a table of all user accounts to be transitioned/disabled.

C.8.2.11 Knowledge Transfer

The Contractor shall describe how knowledge will be transferred from the incumbent staff to the staff of the new contractor (documentation/instruction manuals including as-built documents, formal training classes, one-on-one training/knowledge transfer, etc.).

C.8.2.12 Potential Risks

The Contractor shall discuss what risk management processes based on best practices in industry and government is being applied. The Contractor shall apply risk management at the overall order level as well as for specific network component transition, implementation and operation. The Contractor shall identify all the sources of risk during the transition on period and show what the Contractor will do to mitigate them. The Contractor shall include details on how the Contractor will identify, manage, and reduce risk of schedule delays and service disruption, and provide effective issue resolution and risk mitigation when issues arise.

C.8.2.13 Schedule

The Contractor shall provide a GANTT chart schedule of the transition. The complexity of the transition will dictate the level of detail required in the schedule. However, all major milestones as well as transition start, and completion dates should be included at a minimum. The Contractor shall identify how the transition and implementation of services will meet EPA timelines and milestones including any processes and standards used to ensure meeting agency objectives during the transition. EPA and the Contractor will mutually agree on the final schedule after TO award. The Contractor's schedule shall address the transition, transitioning the optional VMNS described in Section C.7.3.1.7.2 of this SOW at TO award or shortly after award, in parallel transitioning the MTIPS, MPLS WAN, and access circuits, while maintaining connectivity to all applications, and subsequently transitioning the VMNS to IPVS.

C.8.2.14 Handover and Acceptance

The Contractor shall discuss how the customer will formally accept the transition on at the end of the transition. The Contractor shall discuss how they will minimize parallel operations and service disruption to ensure a high-quality customer experience for EPA and all users of the underlying networks interconnected through the provided services.

The Contractor shall implement the EPA approved Transition Plan. The Contractor shall update the Transition Plan throughout the transition period as specific sites and services are scheduled and cut over.

C.8.3 Transition Off Tasks

The Contractor's Role in the Transition Off shall meet the requirements described in C.3.3, C.3.3.1, C.3.3.2, C.3.3.3, and C.3.3.4 Transition Off of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractor's Role in the Transition shall meet the requirements described in C.3.1.2 Contractor's Role in the Transition of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

The Contractor shall address in the Transition Plan the roles and responsibilities of the Contractor in the Transition Off, to include the topics in the plan, property transition of both incumbent and GFE property, intellectual property, user accounts and passwords, knowledge transfers, and risk mitigation.

C.9 Section 508 Requirements/Tasks

C.9.1 Background

The Contractor's Background shall meet the requirements described in C.4.1: Background of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.9.2 Voluntary Product Accessibility Template

The Contractor's Voluntary Product Accessibility Template shall meet the requirements described in C.4.2: Voluntary Product Accessibility Template of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.9.3 Section 508 Applicability to Technical Requirements

The Contractor's Section 508: Applicability to Technical Requirements shall meet the requirements described in C.4.3: Section 508 Applicability to Technical Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.9.4 Section 508 Provisions Applicable to Technical Requirements

The Contractor's Section 508: Provisions Applicable to Technical Requirements shall meet the requirements described in C.4.4: Section 508 Provisions Applicable to Technical Requirements of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.9.5 Section 508 Provisions Applicable to Reporting and Training

The Contractor's Section 508: Provisions Applicable to Reporting and Training shall meet the requirements described in C.4.5: Section 508 Provisions Applicable to Reporting and Training of the *EIS Contract*, as well as any agency-specific requirements detailed in this SOW.

C.9.6 Operating Constraints

The Contractors shall provide details on operational constraints such as infrastructure components that cannot change or must be included in a solution, custom connectivity, agency-specific security considerations or availability requirements that must be met during all phases of the transition in the Contractor's proposal response.

C.10 Technology Refresh Tasks

The Contractor shall develop a Technology Refresh Plan which can accommodate technological advances that occur during the task order period. The plan shall address any software or hardware upgrades that become necessary and specify the process that will be used to upgrade, collect and redistribute hardware or software, if applicable. Additionally, as new technologies are developed and used by the commercial industry or the Government, or as new service types replace obsolete service types, delivery methods, or infrastructure, the Contractor shall identify these technologies and recommend necessary additions, modifications, upgrades, improvements, or replacements. Recommendations should include services or products which are at least equivalent to the existing service. Reviews shall take place on a six-month technology refresh cycle to determine what, if any, technology refresh is required based upon changing technology capabilities, industry and supply chain dynamics, discontinued products, and economic adjustments. The technology refresh may propose alternatives to traditional technology. The EPA anticipates that the cost used during the task order period shall not exceed the cost of the original fixed-price as established in the original agreement unless otherwise stated. However, if there are circumstances that may require price adjustments, which will be in the best interest of EPA, alternatives may be proposed.

Additionally, EPA reserves the right to initiate a technology refresh at any time based on technology innovation that causes changes to the device requirements, such as the need for devices of a different make and model. All proposed technology refreshes shall be submitted and approved for compatibility with mission critical operations and EPA objectives prior to initiation. At no time shall the Contractor substitute or modify any service offering due to a

technology refresh without written authorization from the CO through the issuance of a modification to the contract.

C.11 Program Management Tasks

C.11.1 Meetings

Kick-Off Meeting. The initial kick-off meeting shall be at Research Triangle Park and shall occur within 10 business days after Task Order award. Contractors shall coordinate and provide an agenda and briefing materials to EPA two business days prior to the kick-off meeting.

Monthly Program Meetings. The Contractor shall participate in monthly Program Meetings with EPA technical staff, program managers, and/or executives. The Contractor shall participate in these monthly meetings either in person or via teleconference, at the direction of the OCO or COR. The topics Contractors shall cover at each monthly program meeting include, but are not limited to, service-specific delivery, acceptance, and performance; SLA compliance; invoices and billing detail, adjustments, and disputes; and staffing issues.

Project Review Meetings. The Contractor shall plan and facilitate Project Review Meetings when requested by EPA. The Contractor shall participate in these Project Review Meetings either in person or via teleconference, at the direction of the OCO or COR. The topics Contractors shall cover at each Project Review Meeting include, but are not limited to, the following:

- Review of the most recent Transition Status Report
- Overall project schedule and milestones
- Current risk assessment and mitigation strategies
- Issues and resolution
- Previous action items and status
- Deliverables submitted during the preceding week and upcoming deliverables

C.11.2 Program Management Plan (PMP)

The Contractor shall provide a Program Management Plan (PMP) that describes its approach to managing the awarded EIS services and is IAW EIS Section G.9. The Contractor shall provide a draft PMP with its proposal and a final PMP within 60 calendar days of TO award. The final PMP shall incorporate feedback from EPA. The PMP shall include at minimum:

- Management Approach and Governance Model
- Resource Management
- Risk Management
- Testing Services Verification Test
- Training
- Reporting
- Other items the Contractor deems appropriate

C.11.2.1 Management Approach and Governance Model

The Contractor shall implement and follow industry-standards and proven processes to provide program management services in compliance with Section G.9 of the *EIS Contract*. The Contractor shall provide dedicated support to plan, coordinate, and oversee the transition to the *EIS Contract* and ongoing support for service orders, changes, deletions, and upgrades. The Contractor shall provide program management functions including but not limited to: program control, planning at the task order level, contractor performance, service assurance, reporting and reviews, and senior-level communications.

The Contractor shall provide its management approach and governance model describing how it will balance the need to transition services within schedule constraints and minimize transition risk with the need to transition to transformative technology.

C.11.2.2 Resource Management

The Contractor shall provide Key Personnel as specified below and in Section G.7. These Key Personnel requirements are not to be separately priced but are to be included in the overall service price.

Key personnel shall include:

- Program Manager: Responsible for the Contractor's overall efforts under each Task Order; Must have a PMP certification.
- Transition Manager: See Section C.8
- Network Engineer:
 - Position Description: Network Engineer primary duties shall include maintenance of computer networks, hardware, software, and other related systems, performing disaster recovery operations, protecting data, software, and hardware from attacks, and replacing faulty network hardware components when necessary. You shall also be working closely with the users of our network in order to identify potential issues and fix existing problems. To be a successful candidate, you shall need to have a strong understanding of network infrastructure and network hardware. You shall also need to be able to implement, administer, and troubleshoot network devices including WAPs, firewalls, routers, switches, and controllers. A deep knowledge of application transport and network infrastructure protocols is required.
 - o The Contractor shall be responsible for the following Maintaining and administering computer networks and related computing environments including systems software, applications software, hardware, and configurations.
 - Performing disaster recovery operations and data backups when required.
 - Protecting data, software, and hardware by coordinating, planning and implementing network security measures.
 - Troubleshooting, diagnosing and resolving hardware, software, and other network and system problems.
 - Replacing faulty network hardware components when required.

- Maintaining, configuring, and monitoring virus protection software and email applications.
- Monitoring network performance to determine if adjustments need to be made.
- Conferring with network users about solving existing system problems.
- Operating master consoles to monitor the performance of networks and computer systems.
- Coordinating computer network access and use.
- Designing, configuring and testing networking software, computer hardware, and operating system software.
- Skills and Qualifications:
 - Bachelor's degree in information technology related field of study with a network engineering focus or the equivalent in work experience is required.
 - Strong understanding of network infrastructure and network hardware.
 - Strong understanding and working knowledge of cloud infrastructure and applications.
 - Ability to think through problems and visualize solutions.
 - Ability to implement, administer, and troubleshoot network infrastructure devices, including wireless access points, firewall, routers, switches, controllers.
 - Knowledge of application transport and network infrastructure protocols.
 - Strong understanding and working knowledge of Software Defined Networking (SDN) applications.
 - Ability to create accurate network diagrams and documentation for design and planning network communication systems.
 - Provides specific detailed information for hardware and software selection.
 - Ability to quickly learn new or unfamiliar technology and products using documentation and internet resources.
 - Ability to work with all levels of staff within and outside of IT and outside the organization.
 - A self-starter able to work independently but comfortable working in a team environment.
 - Good analytical and problem-solving skills.
 - Dependable and flexible when necessary.
 - Network security experience.
 - LAN and WAN experience.

In addition, the Contractor shall provide the necessary engineers, telecommunication specialists, technical SMEs, program management support, customer service operations, and billing and ordering support to ensure the highest quality delivery across the EPA enterprise.

The Contractor shall provide a management structure that effectively deploys its resources, including subcontractors, in a manner that ensures a high quality customer experience for EPA users.

C.11.2.3 Risk Management

When manmade, natural, cyber, or other technological events occur, a portion of the Contractor's network may become unusable due to damage. The Contractor shall utilize all

available backup capabilities to maintain network operation while network outages are occurring. The Contractor shall respond to restore full network operation, per *EIS Contract* Section G.8.2. Partial fixes or short-term workarounds may be utilized as part of full system restoration.

The Contractor shall implement a process for identifying program risks, including risks identified in this task order, and actions to mitigate them. The Contractor shall use industry best practices to address ongoing risks, which *include but are not limited to* disaster recovery, continuity of operations, service availability, etc.

The Contractor shall adhere to the service specific SLAs and the service requirements as prescribed in the EIS Section G.8.2.1.1.1 (Service-Specific SLA Table) and EIS Section C for each service included in the Contractor's response to this SOW.

C.11.2.4 Services Verification Testing

The Contractor shall provide an EIS Services Verification Test Plan based on the test methodology defined in EIS Section E.2.2. EIS Services Verification Testing. Accepting or rejecting the services rendered by the Contractor under TOs and service orders shall be in accordance with EIS Section E.2.2. The Contractor shall coordinate corrective actions with EPA and GSA if required.

The Contractor's EIS Services Verification Test Plan shall include a site-specific cut-over plan that requires error free testing IAW each EIS service prior to verification of services and submitting a SOCN to EPA for acceptance.

C.11.2.5 Training

The Contractor shall provide training at no additional cost in accordance with EIS Section G.10. Training includes, but is not limited to, BSS, overall information systems, ordering, billing, inventory, SLA management, trouble ticketing, data exchange, etc.

C.11.2.6 Reporting

The Contractor shall provide all reports as required in the GSA *EIS Contract* if requested by EPA. EPA requires that these reports be able to be downloaded from the Contractor's BSS. EPA also requires that these reports be available in the system only to users who are authorized (by AHC or Task Order). The reports shall also allow for filtering and field customization. In addition, the Contractor shall provide the following:

1. Legacy Transition Off Report: If an awarded Contractor is an incumbent, then it shall produce a monthly report of services moved off of the legacy contracts (Network, WITS3, and LSAs).
2. Usage Reports: Near real time call detail, network traffic detail, reports for usage products and zero usage reports.

C.12 EPA CIO Directives

Where applicable, the Contractors shall conform to the latest version of the Directives issued by the EPA CIO. The EPA CIO Directives can be located at the following website:

<https://www.epa.gov/irmpoli8/current-information-directives>